الجامعة اللبنانية

كلية الحقوق و العلوم السياسية والادارية

العمادة

الدليل الرقمي بين الضابطة العدلية والقضاء : لبنان نموذج

رسالة أعدت لنيل شهادة الماستر ٢ بحثي في القانون الجزائي

إعداد

سامر ابوشقرا

لجنة المناقشة

د. جنان الخوري	الأستاذ المشرف	رئيساً
د. وسام غياض	أستاذ	عضواً
د. سامر سلوم	أستاذ مساعد	عضواً

٢٠٢٠

التصميم

المقدمة:

القسم الأول: حيازة الدليل الرقمي في لبنان

الفصل الأول: جمع الدليل الرقمي: بين الدولة والقطاع الخاص

- المبحث الأول: الأجهزة المخوّلة جمع الدليل الرقمي
- المبحث الثاني: الشراكة مع القطاع الخاص

الفصل الثاني: رفع الدليل الرقمي في ضوء التشريع اللبناني

- المبحث الأول: الصعوبات التي تواجه إجراءات التفتيش
- المبحث الثاني: اعتراض الاتصالات والمراقبة الإلكترونية

القسم الثاني: التحديات التي تفرضها حداثة الدليل الرقمي على القضاء

الفصل الأول: القوة الثبوتية للدليل الرقمي أمام القضاء

- المبحث الأول: قبول الدليل الرقمي من قبل القاضي
- المبحث الثاني: تأثير الدليل الرقمي على سلطة القاضي التقديرية

الفصل الثاني: التعاون الدولي أساس لجمع الدليل الرقمي

- المبحث الأول: تحديد الاختصاص في جرائم المعلوماتية
- المبحث الثاني: أهمية التعاون الدولي في عملية جمع الدليل الرقمي

الخاتمة

المقدمة

تقدم العالم الرقمي وتطورت وسائل التواصل الاجتماعي إلى درجةٍ أصبح من الصعب من دونها استمرار الحياة اليومية، وأصبح أغلب المستخدمين لها، يعيشون محاولين من خلالها رسم الصورة الأمثل والأفضل لهم أمام المستخدمين الآخرين في عالمٍ افتراضي رقمي ينقل الصورة والصوت في حزم بيانات رقمية تنتقل من نظام معلوماتي إلى آخر. وبالتالي أصبح هناك مجتمع إلكتروني شبيه بالمجتمع الذي نعرفه جميعًا. وبالطبع عند الحديث عن مجتمعٍ ما، لا بُدّ من الحديث عن الجريمة وعِلم الإجرام وهذا من الطبيعة البشرية. الّا أنَّ الجريمة هنا في العالم الافتراضي ليست الجريمة التي نعرفها أو نسمع عنها؛ بل هي جريمة معلوماتية إلكترونية (هي نوع حديث إلى حدٍّ ما من الجرائم بالنسبة إلى القوانين التقليدية التي تتناول الجرائم العادية كالقتل والإيذاء والسرقة وغيرها) تحتم بالتالي على الأجهزة الأمنية والقضائية اتباع إجراءات قانونية وتقنية جديدة في المُلاحقة.

ومن أجل إحقاق الحق والعدالة لا بُدّ من مكافحة كلِّ أنواع الجرائم العادية والإلكترونية، عبر أجهزة أمنية جاهزة تُعنى بالتحقيقات وجمع الأدلة اللّازمة لمعرفة الفاعل والمشتركين في الجرم وكشف الحقيقة، وعبر قضاء مختصّ يشرف على التحقيقات ويصدر الأحكام مرتكزاً على وسائل الإثبات القانونية والمقنِعة مثل (الاعتراف، الشهود وغير ذلك) وعلى الأدلة التي ترفع من مسرح الجريمة.

الّا أنَّه ومع التطور التقني العالي، ودخوله جميع تفاصيل الحياة اليومية للأفراد، ظهر نوع جديد من الأدلة وهي الأدلة الرقمية والتي لا يستحصل عليها من مسرح الجريمة الواقعي المحسوس بل من المسرح الافتراضي، حيث تكون البيانات الرقمية مخزنة أو تنتقل من نظام إلى آخر(الحواسيب والآلات والهواتف الخ..) .وهذا النوع من الدليل وضع – رغم أهميته وكثرة انتشاره – الكثير من الصعوبات أمام القضاء والأجهزة الأمنية نظرًا إلى طبيعته الجديدة والحساسة.

وعليه ما هو الدليل الرقمي؟

إنه "ايّة بيانات مخزّنة أو منقولة بواسطة الحاسوب، تدعم أو تدحض أية نظرية ترتبط بكيفية ارتكاب الجريمة، وتتعلق بعناصر هامة في الجريمة "أو" معلومات رقمية مخزنة أو منقولة بشكل يمكن قبوله في المحكمة"[1].

وبالتالي للدليل الرقمي خاصتان أساسيتان: الأولى تشمل المعلومات أو البيانات الرقمية المخزنة في الحاسوب أو المنقوله بواسطته، أيًا كان شكل الحاسوب، بحيث يجوز أن يأخذ شكل الحاسوب الشخصي، أو مخدم الإنترنت (server)، أو الهاتف الجوال أو الكاميرا الرقمية وغيرها، والثانية تتعلق بالقوة الثبوتية لهذه المعلومات والبيانات في اثبات أو نفي الجرائم.[2]

ويمكن القول إن التعامل معه أسهل من التعامل مع الأدلة التقليدية للأسباب التالية:

– يمكن نسخ الدليل الرقمي نسخة طبق الأصل من أجل الحفاظ على النسخة الأصلية وتفادي إتلافها وهذا ما لا يمكن القيام به بالأدلة التقليدية، فلا يمكن صنع نسخة مطابقة عن البصمة أو الشعر.

– إمكانية كشف أي تعديل مقصود أو غير مقصود قد يقوم به الجاني أو المحقق أو الخبير الإلكتروني، من خلال تقنيات وبرمجيات متطورة.

– صعوبة التخلص منه، وهي الميزة الأهم، وهو بذلك يشبه الدليل العلمي المتعلق بالحمض النووي DNA، فإزالة الملفات الإلكترونية عن طريق Delete أو Erase أو حتى اعادة تهيئة القرص الصلب Format وغيرها، لا تشكل عائقاً دون استرجاع هذه الملفات التي ألغيت او أزيلت من الحاسوب.

في المقابل للدليل الرقمي خصائص تجعل التعامل معه أصعب وأكثر تعقيداً من الأدلة التقليدية:

---

[1] عبد الرؤوف الخنّ (محمد) جريمة الاحتيال عبر الإنترنت، الأحكام الموضوعية والأحكام الإجرائية، الطبعة الأولى ٢٠١١، منشورات الحلبي الحقوقية ص ٣٤٠

[2] المرجع السابق ص٣٤٢

١- الطبيعة غير المرئية للدليل الرقمي، أي الطبيعة السيبرانية غير الحسيّة على عكس الأدلة التقليدية، بمعنى أنه بيانات أو حركة اتصالات رقمية تدل في مجموعها على أنماط السلوك الإنساني.

٢- الحجم الكبير للبيانات التي يوجد فيها الدليل الرقمي إذ إن البيانات المتعلقة بالجريمة قد تشكل جزءًا صغيراً من البيانات الموجودة داخل الأقراص الصلبة.

٣- قد يشير الدليل الرقمي أحياناً إلى أشخاص محدّدين لتبيان دورهم في الجريمة الّا أنَّ ذلك يصعب في حالة الجريمة الإلكترونية لأنه يدل على الحاسوب أو نظام المعلومات الذي استخدم ولكنه لا يحدد مستخدمه. وهنا يظهر دور الأدلة التقليدية وخاصةً البصمات.

من هنا تبدأ الإشكالية التي نعالجها في بحثنا والتي تتمحور حول ما مدى قدرة الضابطة العدلية والقضاء في لبنان على التعامل مع الأدلة الرقمية، بدءًا من جمعها إلى حين عرضها أمام القاضي؟ ومدى القوة الثبوتية لهذا النوع الجديد من الإثبات.

يشوب التعاطي مع الدليل الرقمي في لبنان منذ لحظة البدء برفعه من قبل الأجهزة المختصة الى حين عرضه أمام المحكمة واقتناع القضاة به، الكثير من العقبات والصعوبات على الصعيد التقني والتكنولوجي، التشريعي، والقضائي.

على الصعيد التقني، نتناول قدرة الأجهزة الأمنية المعنية بجمع الأدلة في مسرح الجريمة على التعامل مع الأدلة والبيانات الرقمية من الناحية القانونية والتقنية ودور شركات القطاع الخاص في تبادل الخبرات والاستفادة من أصحاب الاختصاص التقني، خاصةً وأن جمع الدليل الرقمي قد يحتاج إلى البحث في ذاكرة الأقراص الصلبة للحواسيب أو إلى اعتراض حزمات البيانات أثناء انتقالها في الوقت الحقيقي للبثّ، وهذا يحتاج إلى قدرات تقنية عالية.

اما الصعيد التشريعي فنعرض من خلاله مدى ملاءمة المواد القانونية الجزائية المتعلقة بالاختصاص وبإجراءات الضبط والتفتيش مع رفع الأدلة الرقمية. وكيفية تطبيق النصوص القديمة ومحاولة تفسيرها من أجل توسيع مفاهيمها لتطال الأدلة الرقمية وخاصةً المواد المتعلقة بإجراءات التفتيش في الجريمة

المشهودة وغير المشهودة. بالإضافة إلى المسؤولية القانونية المترتبة على مزودي خدمات الإنترنت في حفظ الدليل الرقمي وتزويد القضاء المختص به.

اما على الصعيد القضائي فيشكل إلمام القاضي بالعالم الرقمي، الحجر الأساس الذي يتيح له التثبت من صحة الأدلة الرقمية المقدمة له وسلامتها، وتكوين القناعة الصحيحة من أجل إصدار الأحكام العادلة.

لقد أصبح التعاون الدولي أثناء جمع الأدلة الرقمية من القضايا الأكثر أهمية في هذا الموضوع اذ غالباً ما تكون البيانات التي تتعلق بجريمة ما على أرض دولة ما، موجودة على مخدمات وحواسيب في الخارج خاصةً وأن العالم السيبراني هو عالم شاسع، لا حدود جغرافية فيه، والبيانات تتنقل فيه وفق بروتوكول الإنترنت TCP/IP.

من هنا نتساءل عن سبل التعاون الدولي السريع للحصول على الأدلة الرقمية وضمان عدم ضياعها في العالم السيبراني اللا محدود؟

وفق ما أشرنا إليه آنفًا ينقسم بحثنا إلى قسمين: نتناول في القسم الأول دور الأجهزة الأمنية المعنية في جمع الدليل الرقمي حيث نبيّن أهمية الشراكة مع القطاع الخاص في لبنان، والجهود التي بذلت في تطوير النصوص التشريعية، من أجل مواكبة حداثة الدليل الرقمي. وفي القسم الثاني نتناول تحديات القضاء اللبناني في التعامل مع الدليل الرقمي، والحاجة الملحة في للبنان الى تفعيل قنوات التعاون القانوني والقضائي والشرطي الدولي من قبل الدولة اللبنانية، بالإضافة إلى ضرورة الانضمام إلى إتفاقية بودابست للمعاملات الإلكترونية ٢٠٠١ المختصّة، قبل التوصل إلى الخاتمة حيث سنطرح العديد من الإستنتاجات والمقترحات.

القسم الأول: حيازة الدليل الرقمي في لبنان

لم يعد في الامكان الاعتماد فقط على الأجهزة الأمنية التقليدية في مكافحة الجريمة، إذ إن التطور التكنولوجي الرقمي، أصبح على قدرٍ عالٍ من التعقيد والصعوبة للتعامل معه من قبل الأجهزة الشرطية. وأصبح لا مفرّ من استحداث مكاتب جديدة داخل الأجهزة الأمنية قادرةٍ على التعامل مع العالم الرقمي السيبراني ومكافحة الجرائم التي تحصل فيه أو من خلاله، ومع الأدلة الرقمية التي يتم رفعها وحفظها وتقديمها إلى القضاء المختص. وذلك يستدعي خبراتٍ وتقنياتٍ عاليةً لضباط وعناصر الضابطة العدلية والجسم القضائي.

أضف إلى ذلك تفعيلُ تعاونٍ أكثرَ انتاجيةٍ مع القطاع الخاص وأصحاب الاختصاص التقني في العالم الرقمي من أجل الحصول على أدلة رقمية نزيهة وخالية من الشوائب ومقنعة للقاضي حيث يستفاد خبراتهم وقدراتهم التقنية العالية التي قد يرتكز عليها القاضي أحيانًا في إصدار الأحكام هذا من جهة.

ومن جهة أخرى تكمن الفائدة في تنفيذ برامج تعاون وتدريب متبادلة مع ضباط وعناصر الضابطة العدلية وحتى القضاة في سبيل توحيد اتجاهات العمل واللغة الرقمية أثناء التحقيقات.

اضف إلى ذلك، أنه لا يمكن أن تصل خدمة الإنترنت (التي تعدّ الوسيلة الأهم في ارتكاب الجرائم في العالم السيبراني أو للتواصل بين الفاعلين قبل وعند ارتكاب اي نوع من انواع الجرائم التقليدية) إلى المواطنين إلّا من خلال مزودي الخدمات التقنية للإنترنت، الذين لديهم حركة البيانات والاتصالات الرقمية. وبالتالي يبرز دورهم في تزويد الضابطة العدلية والقضاء، عند الحاجة، بكل ما هو مطلوب من حركة بيانات وأدلة رقمية للتسريع في عملية التعرّف على مرتكبي الجرائم وشركائهم وبالتالي إحقاق الحق والعدالة.

لكل ما سبق أهمية كبيرة من الناحية التقنية والعملانية على الأرض، وهي تشكل الحجر الأساس في بداية التكيّف والتعامل مع الجريمة الإلكترونية والأدلة الرقمية.

الّا أنَّ ذلك لا بُدّ له أن يترافق أيضًا مع تعديلات وتطوير في التشريعات الداخلية وخاصةً في مواد قانون أصول المحاكمات الجزائية التي تعنى بإجراءات التفتيش، وضبط الأدلة، والمصادرة، لكي يصبح النص القانوني متماشيًا مع التعقيدات الرقمية الجديدة، إذ إننا لم نعد أمام مسرح جريمة واحد بل أصبحنا أمام عدة مسارحِ جريمةٍ رقمية تكون لأدلة فيها عرضة للاخفاء بشكل سريع أو للتلف، ولم نعد أمام فاعل أو شريك حسي، إنما أمام أجهزة وحواسيب وبروتوكولات إنترنت وعناوين رقمية وأصبح بالتالي من الصعب تحديد الموقع الجغرافي للجهاز الذي ارتكبت عبره الجريمة الرقمية أو الذي يحتوي على الأدلة الرقمية، كما بات تحديد من قام باستخدام هذا الجهاز صعوبة أكثر لتحديد هوية الفاعل وشركائه.

ما هو موقع لبنان في كل سبق؟ هل من مكاتب متخصصة في جمع الدليل الرقمي؟ هل من دور للقطاع الخاص و مزودي الخدمات؟ و ماذا عن تشريعاته؟

نشرح في الفصل الأول التفاعل بين الأجهزة الأمنية والقطاع الخاص لخلق شراكة فعالة في لبنان. وفي الفصل الثاني ننتقل إلى مناقشة التشريعات اللبنانية في مجال جمع الدليل الرقمي ومدى تلاؤم هذه التشريعات مع العالم الرقمي وجرائم المعلوماتية.

الفصل الأول: جمع الدليل الرقمي: بين الدولة والقطاع الخاص

إن العمل الشرطي في مجال الضابطة العدلية والتحقيقات الأولية التي تجريها النيابة العامة في الجرائم، يحتاج إلى تطويرٍ دائمٍ وفقاً لتطور النية الجرمية وتطور وسائل ارتكاب الجرائم. ففي الجرائم التقليدية كالقتل والسرقة والإيذاء، المشهودة منها وغير المشهودة، تسعى الضابطة العدلية والنيابة العامة إلى حماية مسرح الجريمة والبدء برفع الأدلة والاستماع الى الشهود وتوقيف المشتبه فيهم وغيرها من الإجراءات التي من شأنها تبيان الحقيقة، وبالطبع لا بُدَّ من إرسال الأدلة المرفوعة إلى مختبرات تقنية من أجل تحليلها والوصول إلى النتيجة المطلوبة، كخطوة إضافية نحو تحديد فاعل الجريمة وشركائه. ولكن ليس جميع ضباط وعناصر الأجهزة الأمنية مدرّبين بالشكل التقني اللازم على رفع الأدلة الرقمية أو على تحليلها في المختبرات، لذلك تلجأ هذه الأجهزة إلى التعاون مع مدنيين، شركات كانوا أم اشخاصًا، وهم أصحاب الاختصاص التقني اللازم من أجل الاستفادة من خبراتهم، كما وتلجأ إلى إعداد الكادر البشري الشرطي عبر دورات تدريبية مستمرة في مجال العالم الرقمي وضبط الأدلة الرقمية.

إن ذلك لا يمكن أن ينفذ من دون إشراك القطاع الخاص (أفراد وشركات) في هذه العملية خاصةً وإن الوصول إلى العالم الرقمي يتم في مُعظمِه من خلال مزودي الخدمات التقنية.

وفي لبنان رغم التقصير الحاصل بعض الشيء في هذا المجال الّا أنَّنا نرى نيّة جديّة لدى القضاء والقوى الأمنية في الاستعداد المتواصل من أجل التعامل مع العالم الرقمي وإضفاء نوع من الأمن السيبراني والثقة بأن الدولة مسيطرة على العمليات الرقمية الاقتصادية والتجارية والأمنية والاجتماعية التي تحصل من خلاله أو فيه. وسنتناول في ما يلي المكاتب التي استحدثت في قوى الأمن الداخلي من أجل التعامل مع الأدلة الرقمية في الجرائم التقليدية وجرائم المعلوماتية لننتقل بعدها إلى الدور الذي أعِطي للقطاع الخاص في لبنان، من أجل مساعدة القضاء والضابطة العدلية في رفع الدليل الرقمي في الجرائم.

<u>المبحث الأول</u> : الأجهزة المخوّلة جمع الدليل الرقمي

إن الجهاز المعني بجمع الأدلة والحفاظ على مسرح الجريمة هو القوى الأمنية وبالأخص قوى الأمن الداخلي، من خلال تطويق مسرح الجريمة وعزله وعدم لمس أي شيء إلا من قبل متخصّصين. وذلك ينطبق ايضًا على الأدلة المرفوعة في العالم الإلكتروني (جريمة إلكترونية أم عادية) حيث تظهر جليًا أهمية الإجراءات التي تتخذها القوى الأمنية أثناء الدخول في ذاكرة الحواسيب أو الهواتف أو إلى العالم السيبراني ورفع الأدلة الرقمية المتاحة بكل احترافية ودقة لأن أي خللٍ أو خطأ في العملية قد يؤدي إلى إتلاف الدليل وعدم القبول به أمام المحكمة.

إن زيادة الانتاجية والاحترافية في التعاطي مع الأدلة الرقمية يستوجب إمكانيات مادية تقنية وبشرية كبيرة. فالأجهزة الإلكترونية التي يجب ان تتوفر باهظة الثمن، والبرامج الرقمية كثيرة التعقيد، والتدريب عليها يحتاج وقتًا وطاقةً بشريةً كبيرةً. وهذا ما يجعل الأمر أكثر صعوبة في الواقع اللبناني حيث الإمكانيات المادية محدودة، وبالتالي هناك نقص في التجهيزات التقنية والبرامج. ويبقى الإتكال على الطاقات البشرية اللبنانية التي مازالت حتى الآن تبذل جهدًا جبارًا نظراً إلى الامكانيات المحدودة المتاحة مقارنةً بإمكانيات الدول الأخرى مثل فرنسا والولايات المتحدة.

البند الأول: قوى الأمن الداخلي والدليل الرقمي

بعد حماية مسرح الجريمة من قبل القوى الأمنية الموجودة على الأرض يعمل مكتب الحوادث التابع لقسم المباحث الجنائية العلمية في الشرطة القضائية على رفع الأدلة التقليدية الموجودة في مسرح الجريمة (بصمات، أسلحة، عينات من الحمض النووي، الخ...) واعداد بياناتها وحفظها من أجل نقلها إلى المختبرات الجنائية حيث يصار إلى تحليلها ودراستها ومعرفة مدى ارتباطها بالفاعل أو بالمشترك في الجريمة. إلّا أنَّ التطور الرقمي الذي يحصل في جميع الميادين، فرض نفسه على القوى الأمنية، التي أصبحت في غالبيتها، تقسّم الأدلة المرفوعة من مسرح الجريمة إلى نوعين: نوع رقمي ونوع عادي.

لذلك، وفي خطوة جيدة جرى في سنة الفين وستة عشر تجهيز المباحث العلمية بمختبر جنائي رقمي متخصص في معالجة الأدلة الرقمية و تحليلها وانشئت فروع جديدة في **مكتب الأعتدة واللوازم** من أجل تفعيل التعامل مع الأدلة الرقمية : فرع الحواسيب – فرع الهواتف الذكية – فرع الصوت – فرع الفيديو و الصورة – فرع الشرائح الإلكترونية.

وتكون مهام هذا المكتب معالجة، وتحسين التسجيلات الصوتية والصورة والفيديوهات الرقمية التي تستخرج من الكاميرات الرقمية، استخراج وتحليل الاثار القانونية الرقمية الموجودة في جميع الأنظمة الرقمية.[٣]

وكانت مؤسسة قوى الأمن الداخلي قد استحدثت سابقاً "**مكتب مكافحة جرائم المعلوماتية والملكية الفكرية**" بموجب مذكرة خدمة صادرة عن المديرية العامة لقوى الأمن الداخلي عام ٢٠٠٦، وألحق بقسم المباحث الجنائية الخاصة في الشرطة القضائية. لم تحدَدَ مهام هذا المكتب بشكل قانوني واضح حتى الآن بسبب عدم تعديل القانون١٧ الذي ينظم ويحدد مهام قوى الأمن الداخلي.

و لكن يمكن القول أن مهام المكتب تكون منبثقة من المهام المحددة لقسم المباحث الجنائية الخاصة عمومًا:

وهي تتبع وقمع الجرائم الماسة بأمن الدولة، ومنها النيل من هيبة الدولة والشعور القومي، وإثارة الفتن، والإرهاب والجرائم التي تنال من الوحدة الوطنية، الجرائم المالية ومنها جرائم التزوير المالي وتزييف العملة، والإفلاسات الاحتيالية والشركات الوهمية والمضاربات غير المشروعة وجرائم تقليد العلامات الفارقة للصناعة والتجارة وجرائم تبييض الأموال، والجرائم المعتبرة هامة إن كان على صعيد مرتكبيها أو على صعيد الوسائل المستعملة في ارتكابها أو للصدى أو التأثير الهام الذي تتركه على الرأي العام.

---

[٣] مذكرة الخدمة في قوى الامن الداخلي رقم ٢٠٤/٢٤٦ش٢ تاريخ١/١١/٢٠١٦

يتالف هذا المكتب من ضباط وعناصر من أصحاب الاختصاص أو من عناصرَ خَضعوا لدورات تدريبية مكثفة في هذا المجال. ولقد اظهر هذا المكتب، رغم نقص الإمكانات التقنية، نتائج إيجابية في العديد من الجرائم.

ولقد أصدرت محكمة التمييز سنة ٢٠١٤[٤] قرارًا اكدت فيه صلاحية المكتب المذكور، بعد أن طلب المستأنِف "فسخ القرار المستانف لبطلان التحقيق الاولي من قبل مكتب مكافحة جرائم المعلوماتية وحماية الملكية الفكرية في لبنان ذلك ان الغاية من إنشاء هذا المكتب تكمن في فهم التقنيات المعلوماتية وعمله يقتصر على الخبرة التقنية والفنية ولعبه دور الضابطة العدلية وبالتالي إن إجراء التحقيقات وفي جرائم المعلوماتية يعدّ تجاوزًا لمهامه".

واعتبرت المحكمة ان هذا المكتب هو من الشرطة القضائية التي تساعد النيابة العامة في استقصاء الجرائم، وتكون التحقيقات التي جرت بواسطته مستوفية الشروط القانونية وصدقت القرار المستانف.

و من ناحية أخرى تم استحداث **الفرع الفني في شعبة المعلومات،** ولقد حققت هذه الشعبة من خلاله إنجازات غير مسبوقة على الصعيد الوطني عبر كشف شبكات كبيرة من جواسيس وعملاء العدو الصهيوني، مستخدمة التقنية العالية الرقمية والخبرات الكبيرة لضباطها وعناصرها من خلال تحليل الاتصالات الرقمية وحركة البيانات في الأنظمة، وتحديد الموقع الجغرافي للمجرمين عبر ملاحقة البث الرقمي والاتصالات.

وبعيدا عن السياسة ومشاكلها، سمح لهذه الشعبة بالوصول إلى داتا الاتصالات[5] اللّازمة من أجل مكافحة الجريمة العادية والرقمية، وهي تحتوي على بيانات مفصلة عن حركة الاتصالات لشخص ما

---

[٤] محكمة التمييز، الغرفة التاسعة، قرار رقم ١ تاريخ ٢٠١٤/١/٩ ،جان عاصي/الحق العام.

[5] تحتوي داتا الاتصالات على بيانات مفصّلة عن حركة الاتصالات وعن كل رقم خلوي، الفاتورة المفصلة إضافة إلى معطيات، تصنف تقنية إلى حد ما، لا يستطيع المواطن العادي تحليلها لأنها مرتبطة بمعطيات فنية تتعلق بمحطات شبكة الهاتف الخلوي.

فتحتوي داتا الاتصالات أقله على البيانات التالية: رقم الخط الخلوي، صاحب الخط، الرقم التسلسلي للهاتف، نوع الاتصال (رسالة نصية، صوت...) تاريخ الاتصال، وقت الاتصال، الرقم المتصل، مدة الاتصال، الرقم الذي اتصل،

وعن كل رقم خلوي، والفاتورة المفصلة، إضافة إلى معطيات تُصنف تقنية إلى حد ما، لا يستطيع المواطن العادي تحليلها، لأنها مرتبطة بمعطيات فنية تتعلق بمحطات شبكة الهاتف الخلوي.

هذه البيانات البسيطة تساعد كثيرًا على أرض الواقع في فهم ما يجري في الوطن من مكالمات طبيعية ومكالمات غير طبيعية وتساعد كثيرًا في تتبع أثر من يخطط لعمليات تطال أمن المواطنين. ولقد تمكن النقيب الشهيد المهندس وسام عيد من الوصول إلى تحديد الأرقام الخلوية التي يشتبه في أنها استخدمت في اغتيال دولة الرئيس رفيق الحريري، ولقد ارتكزت المحكمة الدولية الخاصة بلبنان على هذه الأدلة الرقمية بالتحديد. وهذا يؤكد على أن ميزة لبنان تكمن في طاقته البشرية الذكية التي رغم الامكانات المحدودة يمكن أن تصل إلى نتائج كبيرة ومهمة.

البند الثاني: الأجهزة المعنية بجمع الأدلة الرقمية في فرنسا والولايات المتحدة

تشكل فرنسا والولايات المتحدة مع اختلاف المدارس القانونية للإثنتين (لاتينية وانغلوساكسونية) نموذجًا مهمًا في إطار التعاطي مع جريمة المعلوماتية وضرورة خلق مكاتب أمنية جديدة داخل أجهزة الشرطة من أجل رفع الأدلة الرقمية:

ففي فرنسا أُنشيء سنة ١٩٩٤ مركز سرية التحقيقات بشأن الغش في تكنولوجيا المعلومات (BEFTI).

La Brigade d'Enquête sur les Fraudes aux Technologies de l'Information

وهو جهاز معنيّ بمكافحة الجريمة الرقمية تحت إدارة الشرطة في باريس ويكون نطاق عملها في باريس فقط، وقوة هذا الجهاز تكمن في كونه الوحيد القادر، دون الخروج من مكاتبه أن يلاحق الجرائم الرقمية ويتعرف الى أي مستخدم مشتبه به على الإنترنت من خلال استخدام حواسيب محمولة صغيرة قادرة على التعرف الى العناوين الرقمية في أقل من خمس دقائق، كما يقوم بمهام

إسم المحطة المرتبط بها الرقم أثناء اجراء المكالمة، إسم المحطة المرتبط بها الرقم الآخر، الرقم التسلسلي للهاتف الرقم الآخر.

تربوية من خلال اضطلاعه بإعلامِ المؤسسات الخاصة والعامة المشتبه مواجهتها لمشاكل الغش المعلوماتي[6]. كما ويقوم بتقديم المساعدة التقنية اللازمة للشرطة القضائية، كما وله الحق في الاستعانة بمهندسين تقنيين بعد موافقة القضاء.

كما وبعد إقرار قانون GODFRAIN[7] المتعلق بالغش المعلوماتي وجرائم المعلوماتية سنة ١٩٨٨ أنشيءَ المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات.

l'Office Central de lutte contre la Criminalité Liée aux Technologies de l'Information et de la Communication.(OCLCTIC)

و يعمل هذا المكتب تحت إدارة الشرطة القضائية ويشمل نطاقه كل فرنسا، ويعنى بالتنسيق الدائم مع الإنتربول واليوروبول ونظام الشنغن. وهو كما الجهاز الذي سبق، يكون معنيًا بمكافحة الجريمة الرقمية الإلكترونية وخاصةً تجارة الممنوعات والجرائم المالية غيرها....ولقد قسّمت المهام فيه إلى ثلاثة أقسام: القسم الأول تكون مهامه مركَّزة على الجرائم المرتبطة بحماية الملكية الفكرية، والقسم الثاني تكون مهامه مرتبطة بانظمة الاتصال ونقل البيانات اما القسم الثالث فتكون مهامه مرتبطة تقديم الدعم اللازم لأي جهاز آخر في ما يختص بالإجراءات التقنية لرفع وحفظ الأدلة الرقمية.[8]

كما عملت الدولة الفرنسية على تطوير أجهزة كانت تعنى بالأصل بجمع الأدلة، مثل معهد التفتيش الجزائي للشرطة الوطنية (L'Institut de Recherche Criminelles de la

[6] الخوري (جنان)، الجرائم الاقتصادية الدولية والجرائم المنظمة العابرة للحدود، الطبعة الأولى، مكتبة صادر ناشرون، سنة ٢٠٠٩ ص ٣٢٣.

[7] Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique.

[8] Chaer (Nidal),**La Criminalité informatique devant la justice penale,** édition juridique sader 2004, Beirut, Liban page 206.

(Gendarmerie Nationale) بحيث جرى تدريب الضباط والعناصر على كيفية التعامل مع الأدلة الرقمية من حيث الجمع والحفظ بالشكل العلمي الدقيق.[9]

أما في الولايات المتحدة، فلقد أُنشئت عدّة أجهزة متخصّصة:

- شرطة الويب WEB POLICE ، وهي نقطة مراقبة على الإنترنت، وملاحقة الجناة والقراصنة، وتلقّي الشكاوى من المستخدمين، والبحث عن الأدلة الرقمية وحفظها الى حين عرضها أمام المحكمة.
- مركز تلقّي شكاوى جرائم الإنترنت IC3 الذي انشيء من قبل مكتب التحقيق الفيدرالي FBI ويتلقى هذا المركز الشكاوى عبر الإنترنت من خلال استمارة إلكترونية يعمل متخصصون في هذا المركز على تحليل الشكاوى وربطها بالشكاوى الأخرى ليصار بعدها إلى إحالتها للجهات المختصة.[10]

والملفت في الولايات المتحدة إنشاء نيابة عامة خاصة بجرائم الحاسوب والاتصالات CTC[11] وتتكون من قضاة تلقوا تدريباً مكثفاً على معالجة بيانات الأنظمة الرقمية، ومنحوا الحق الاستعانة بأي مكتب مختص بجرائم المعلوماتية والأدلة الرقمية بالتنسيق مع قسم جرائم الحاسوب والتعدّي على حقوق الملكية الفكرية، والمركز الوطني لحماية البنية التحتية التي قد تكون عرضةً لهجومات واعتداءات عبر الإنترنت وخاصةً شبكة الاتصال بين المصارف.

نلاحظ مدى الاهتمام الكبير في مثل هذه الدول بجريمة المعلوماتية والإنترنت والدليل الرقمي.

---

[9] خوري (جنان)، **مكافحة جرائم المعلوماتية**، تحديات وافاق، المؤتمر الاقليمي الأول، الطبعة الأولى ٢٠١٥،دائرة المنشورات في الجامعة اللبنانية ص ٢٦٣.

[10] عبد الرؤوف الخنّ (محمد) **جريمة الاحتيال عبر الإنترنت**، الأحكام الموضوعية والأحكام الإجرائية، الطبعة الأولى ٢٠١١، منشورات الحلبي الحقوقية ص ٣٢٣.

[11] وهو اختصار لComputer and Telecommunication Coordinator

وكل هذه الأجهزة التى ذكرناها، خير دليلٍ على اعتراف هذه الدول بأن العالم الرقمي أصبح أكثر ارتباطًا بالجريمة عما كان في الماضي حيث لا بُدّ من التعاطي معه باحترافية أعلى وتخصصٍ أدقّ نظرًا إلى التطور الدائم الذي يشهده العالم الرقمي.

المبحث الثاني الشراكة مع القطاع الخاص

من يود الاستفادة من موارد شبكة الإنترنت، يجب أن يكون موصولًا بها أولاً. وهنا برز نوع جديد من المهن، وهي تأمين خدمات الاتصال بشبكة الإنترنت، يتولاها موردون مستقلون يعرفون بموزّعي الخدمات التقنية. بالفرنسية fournisseurs d'accés وبالإنجليزية internet service providers أو (isp) [12]. ومع ازدياد الحاجة إلى شبكة الإنترنت والبيانات الرقمية عليها ظهر نوع آخر وهو مستضيف البيانات أو le fournisseur d'heberjement الذي يكون دوره حفظ المعلومات والبيانات الرقمية بناءً على عقد يُبرم بينه وبين المشترك بشكل مدفوع أو مجاناً وأبرز مثال على ذلك شركة GOOGLE التي تسمح مثلًا وبشكلٍ مجاني حفظ البيانات لأي مُنتسب شرط تسجيل الدخول إلى الشبكة الخاصةً بها من خلال البريد الإلكتروني.

ينبثق دور القطاع الخاص في جمع الأدلة الرقمية من دوره في تزويد المستخدمين بخدمة الإنترنت على الأراضي اللبنانية، فغالبًا ما تكون كل الآثار التي يتركها المجرمون مسجلة عند مزودي الخدمات التقنية، وهنا يكمن الدور الأساسي حيث لا بُدّ من التعاون الكامل مع أجهزة الدولة الأمنية والقضائية من أجل ضمان عدم ضياع الأدلة الرقمية. من هذا المنطلق، نطرح هنا مسألتين: **الأولى** هي ماذا إذا كان توريد الخدمات يحتاج إلى ترخيص مسبق من السلطات الرسمية؟ أم أن ذلك يشكل أمرًا غير مقيّد ومتاح لأي شخص. **والمسألة الثانية** هل التعاون مع الأجهزة الأمنية ومع موزع الخدمات التقنية (ISP) يكون من باب حسن النية أم من خلال قوانين واضحة ملزمة في حالات محددة وتحت طائلة المحاسبة القانونية؟

---

[12] عيسى(ميشال)، **التنظيم القانوني لشبكة الإنترنت،دراسة مقارنة في ضوء القوانين الوضعية والإتفاقيات الدولة**،الطبعة الأولى٢٠٠١، المنشورات الحقوقية صادر ص ٨٣

البند الأول: مسؤولية مزودي الخدمات التقنية في لبنان

على عكس القوانين الأميركية[١٣]، حيث لا تخضع خدمة تأمين الاتصال بالإنترنت لترخيص مسبق وجعل لجنة الاتصالات الفدرالية مسؤولة عن تنظيم العملية[14]، جعل لبنان مورّدي الخدمات التقنية خاضعين لترخيص مسبق من قبل "الهيئة المنظمة للاتصالات".

هذه الهيئة مؤسسة عامة مستقلّة، جرى تأسيسها بموجب القانون ٤٣١/ ٢٠٠٢، وأُنيط بها تحرير وتنظيم وتطوير قطاع الاتصالات في لبنان. باشرت الهيئة بعملياتها بعد تعيين مجلس إدارتها في شهر شباط٢٠١٧. تشجّع الهيئة الاستثمار، وتحافظ على استقرار السوق في المواضيع المتعلقة بالاتصالات. وهي تصدر التراخيص والأنظمة والقرارات، وتتولى إدارة الترددات والاتصالات وغيرها وقد أنيط بها إعطاء التراخيص اللّازمة لمزودي الخدمات التقنية.[15]

---

[13]United States Communications Act of 1934 Code

Title 47 – TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS

CHAPTER 5 – WIRE OR RADIO COMMUNICATION

§151:For the purpose of regulating interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all the people of the United States, without discrimination on the basis of race, color, religion, national origin, or sex, a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of the national defense, for the purpose of promoting safety of life…"

[14] عيسى(ميشال)، **التنظيم القانوني لشبكة الإنترنت، دراسة مقارنة في ضوء القوانين الوضعية والإتفاقيات الدولة**،الطبعة الأولى٢٠٠١، المنشورات الحقوقية صادر ص٨٩.

[15] http://www.tra.gov.lb(last revision 23/12/2019)

و في هذا السياق تم طرح مشروع لنظام التراخيص الممنوحة لمقدّمي الخدمات من قبل هيئة الاستشارات العامة في ٣٠ نيسان ٢٠٠٧ وحددت المهلة النهائية قبل ٣٠ حزيران ٢٠٠٧. وبعد الأخذ بعين الاعتبار آراء ومقترحات المعنيين، اقر مجلس إدارة الهيئة مشروع نظام التراخيص الممنوحة لمقدّمي الخدمات في٢٠٠٩/٤/٢٧ أحيل هذا النظام إلى وزير الاتصالات لإحالته إلى مجلس الشورى لإبداء الرأي فيه.

يتضمن مشروع "نظام التراخيص الممنوحة لمقدّمي الخدمات" توضيحات مرتبطة بتدابير "الهيئة المنظمة للإتصالات" في ما يتعلق بالترخيص لمقدّمي الخدمات وكيفية التعامل مع كلّ أنواع التراخيص الممنوحة لهم، وهو يوفر لهم أيضًا إطار عمل خاص يتكيّف مع احتياجاتهم. وتفصِّل هذه الوثيقة أنواع وتصنيف التراخيص التي تصدر عن الهيئة. كما أنها تعرض كل الشروط التي تُمنح الرخص بموجبها، فضلاً عن عملية إصدارها.

ولقد نفّذت الهيئة المنظمة للاتصالات بمؤازرة من مكتب مكافحة جرائم المعلوماتية في قوى الأمن الداخلي، مداهمات لمراكز موزّعي خدمات الإنترنت غير المرخّصة والتي تسبب تشويشاً على وصلات الربط الميكروية الثابتة التي تشغلها وزارة الاتصالات في منطقة "زغرتا" وجوارها، وكذلك جرى الكشف على مركز إحدى الشركات غير المرخص لها في منطقة "جونية" التي تقوم تزود محطات فضائية لموزعي القنوات الفضائية بالكابل وذلك بواسطة شبكات كابلات نحاسية وألياف ضوئية وخطوط ربط الميكروية غير المرخصة، وقد أُبلغ أصحاب هذه المراكز بضرورة الحضور إلى مديرية قوى الأمن الداخلي- مكتب مكافحة جرائم المعلوماتية للاستماع إلى إفادتهم لاتخاذ الإجراءات القانونية المناسبة بحقهم.[16]

ويتبين أنَّ تأمين خدمة الإنترنت ليست حرةً في لبنان بل يخضع لنظام تراخيص محدد، وهذا يسهل على الأجهزة الأمنية والقضاء عملية ايجاد الأدلة الرقمية المتعلقة بحركة الاتصالات والبيانات الرقمية.

[16] http://www.tra.gov.lb/NewsDetailsar.aspx?pageid=1786 (last revision 23/12/2019)

يبقى سؤال ما هي المسؤولية التي تترتب على مزودي الخدمات التقنية أثناء إجراءات التحقيق ورفع الأدلة الرقمية، وهل من واجب عليها يفرض التعاون في سبيل حفظ البيانات الرقمية وإتاحة الوصول إليها؟

لم يكن في لبنان من قانون ينظم المسؤولية التي تقع على عاتق مزودي الخدمات التقنية، لغاية صدور القانون رقم ٨١ تاريخ ١٠-١٠-٢٠١٨ الذي تناول في القسم الثالث منه الأحكام القانونية المتعلقة بالنقل إلى الجمهور بوسيلة إلكترونية، أي موجبات مقدمي الخدمات التقنية (مقدم خدمة الاتصال أو مستضيف البيانات). ولقد اشتمل القانون على النقاط التالية:

- أعفى القانون مقدّم خدمة الاتصالات ومستضيف البيانات من مراقبة البيانات الرقمية التي ترسل من خلاله أو تخزن مؤقتًا في نظامه الرقمي. ولكنه في المقابل فَرض عليه أن يسحب هذه المعلومات و البيانات أو أن يجعل الوصول إليها مستحيلًا إما بناء على طلب من مرسل المعلومات أو من السلطة القضائية، أو تلقائيًا إذا تأكد من طابعها المشروع.[17] وهنا لم يطلب القانون من مقدم الخدمات البحث والتدقيق في مشروعية هذه البيانات، بل يقوم هذا الموجب اذا كانت عدم المشروعية ظاهرة بشكل واضح وجلي.
- ألزم القانون مقدمي الخدمات بحفظ المعلومات التي تحدد هوية كل مشترك وبحفظ حركة البيانات الرقمية (وليس المحتوى كما سنشرح لاحقًا) لمدة ٣ سنوات. وهنا لا بُدّ من تسجيل بعض الملاحظات:

---

[17] **المادة ٦٩ تاريخ بدء العمل: ٢٠١٨/١٠/١٠**: لا يُلزم مقدم خدمة الاتصال بمراقبة المعلومات التي يرسلها او التي يخزنها مؤقتاً. انما يتوجب عليه فوراً، تحت طائلة المسؤولية، ان يسحب المعلومات المخزّنة مؤقتاً او أن يجعل الوصول اليها مستحيلاً بناء على طلب مرسل المعلومات او بناء على قرار من السلطة القضائية.

المادة ٧٠ تاريخ بدء العمل: ٢٠١٨/١٠/١٠: لا يُلزم مستضيف البيانات بمراقبة المعلومات التي يخزنها من اجل وضعها في تصرف الجمهور، انما تترتب عليه المسؤولية إذا لم يسحب هذه المعلومات او إذا لم يجعل الولوج إليها مستحيلاً فور معرفته الفعلية بطابعها غير المشروع الظاهر جلياً.

انتشر في الآونة الأخيرة مزودو خدمات إنترنت بشكل غير منظم وغير مشروع، ما صعّب على الضابطة العدلية التعرف إلى هوية المستخدمين الذين يرتكبون الجرائم عبر الإنترنت أو إلى الحصول على حركة البيانات التي تعتبر من الأدلة الرقمية المهمة. وبالتالي يلزم هذا القانون (ولو بشكل غير مباشر) مزودي الخدمات تسجيل التفاصيل المتعلقة بهوية المشترك من خلال طلب هويته وحفظها، وهذا أمر جيد. ولكن يجب أيضًا تسجيل التفاصيل المتعلقة بعنوان سكنه وبريده الإلكتروني والتأكد من صحة هذه المعلومات من خلال إرسال بطاقات مكشوفة مع اشعار بالاستلام إلى عنوان سكنه وبرسالة إلى بريده الإلكتروني وعدم تفعيل الخدمة إلا بعد جواب الذي يريد الاشتراك. فبهذه الطريقة نضمن قدرة الضابطة العدلية أو القضاء على الوصول إلى صاحب البيانات فورًا من دون عناء من خلال مزودي الخدمات، وهذا ما لم يقرّه القانون.

- سمح القانون للضابطة العدلية، وبعد أخذ إشارة القضاء، أن يطلب من مزود الخدمة الحفاظ على بيانات رقمية إضافية أو محددة لمدة ٣٠ يومًا، وعلى الأخير أن يلتزم بذلك وأن يقدّم كل سبل التعاون.

  ولكن حرصاً على الحفاظ على خصوصية البيانات والمعلومات الشخصية وخوفاً من تعسف الضابطة العدلية في استخدام هذه السلطة، منع القانون تسليم هذه المعلومات التي تم حفظها إلى الضابطة العدلية إلا بعد قرار واضح من المرجع القضائي المختص.

- أضف إلى ما سبق، لم يشمل القانون محتوى أو مضمون البيانات بل اقتصر فقط على حركة البيانات لما في ذلك من ضمان لحرية التعبير وخصوصية الأفراد والإبقاء على ديمقراطية النظام وعدم تحوله إلى نظام قمعي، وسوف نفصل ذلك أكثر في المبحث الثاني من الفصل الثاني.

- لا يمكن التذرّع بالسرية المهنية والعطل التقني لعدم تزويد القضاء والضابطة العدلية بما هو مطلوب تحت طائلة الحبس.[18]

- على مزود الخدمة أن يخوِّل الوصول إلى المعلومات المذكورة وفقاً للوقت الحقيقي (real time) لأي عملية اتصال عابرة عبر شبكته.[19]

---

[18] **المادة ٧٢ تاريخ بدء العمل: ٢٠١٨/١٠/١٠:** على مقدّم الخدمات التقنية حفظ المعلومات المتعلقة بحركة البيانات لجميع الأشخاص الذين يستعملون خدماتهم، والتي **تمكّن من تحديد هوية هؤلاء**، وكذلك البيانات التقنية الأخرى للاتصالات، وذلك لمدة ثلاث سنوات تسري اعتباراً من تاريخ تنفيذ الخدمة.

للضابطة العدلية في اطار إجراءات تحقيق في دعوى جزائية،وبعد إعلام المرجع القضائي المختص، الطلب من مقدمي الخدمات التقنية حفظ بيانات تقنية إضافية لما هو منصوص عليه في الفقرة الأولى من هذه **المادة لمدة اقصاها ثلاثين يوماً** وبشأن واقعة محددة وأشخاص محددين، وذلك بالنظر إلى طابع العجلة وإمكانية تعرّض هذه البيانات للفقدان او التعديل. **لا تسلم هذه البيانات إلى الضابطة العدلية إلّا بقرار من المرجع القضائي المختص.**

لا يجوز لمقدم الخدمات التقنية التذرع بأي خلل تقني يؤدي إلى عدم حفظ البيانات التقنية، ويُلزم باتخاذ التدابير التقنية الملائمة التي تحدد بقرار من وزير الاتصالات.

تخضع البيانات التقنية للسرية المهنية المُلزم بها مقدم الخدمات التقنية. لكن لا يمكن له التذرع بهذه السرية بوجه القضاء المختص، وذلك في حدود مقتضيات التحقيقات والمحاكمات.

لا يشمل موجب الحفظ المنصوص عليه في الفقرة الأولى المحتوى او المضمون المخزن او المنقول والمعبر عن افكار الشخص مؤلفها، كالمراسلات المتبادلة او محتوى المعلومات او المواقع المخزنة او المنقولة.

[19]**المادة ٧٦ تاريخ بدء العمل: ٢٠١٨/١٠/١٠:** على مقدمي الخدمات التقنية التعاون مع القضاء المختص والمراجع المنصوص عنها في القانون رقم ٩٩/١٤٠ وضمن حدود إظهار الحقيقة في كل تحقيق يجريه أو في كل دعوى عالقة أمامه.

للقضاء المختص والمراجع المنصوص عليها في القانون رقم ١٤٠/٩٩ وضمن حدوده، في اطار تحقيق او دعوى، ان تُلزم مقدم الخدمات التقنية بتسليمها البيانات التي في حوزته أو الموضوعة تحت رقابته، تنفيذاً لموجبي الخط المنصوص عليهما في المادتين ٧٢ و٧٤ من هذا القانون، وذلك في حدود مقتضيات التحقيقات والمحاكمات.

البند الثاني: دور الخبرة التقنية.

"الخبرة التقنية هي إبداء رأي فني من شخص مختص فنياً. في شأن واقعة ذات أهمية في الدعوى الجزائية "[20].

للسلطات القضائية في لبنان الحق في تعيين الخبراء عند الضرورة. وللنائب العام أن يستعين بخبير أو أكثر في الجناية المشهودة وخارجها للتدقيق في الشكاوى أو الاخبار أثناء التحقيق الأولي للاستعانة بخبراتهم التقنية.[21] ولقد ترك المشرع المساحة الكافية ولم يحدد نوع الخبرة. لذلك لا مانع في القانون من الاستعانة بخبراء في العالم الرقمي من أجل التحقق من صحة الأدلة الرقمية وتقديم المساعدة للقضاة.

على مقدم الخدمات التقنية، بناءً لقرار المرجع القضائي المختص أو المراجع المنصوص عليها في القانون رقم ١٤٠/٩٩ وضمن حدوده، ان يزوده فوراً بالمعلومات المتعلقة بحركة البيانات وبالبيانات التقنية الاخرى المنصوص عليه في المادتين ٧٢ و٧٤ من هذا القانون، وان يخولها الوصول إلى المعلومات المذكورة وفقاً للوقت الحقيقي (real time) لأي عملية اتصال عابرة عبر شبكته.

[20] حسني (نجيب)،شرح قانون العقوبات القسم العام ، الطبعة الثالثة ٢٠٠٠ ، منشورات الحلبي الحقوقية بيروت لبنان ص ٤٧٤.

[21] **المادة ٣٤ أ.م.ج تاريخ بدء العمل: ٢٠٠١/٠٨/٠٢:** إذا استلزمت طبيعة الجريمة أو آثارها الاستعانة بخبير أو أكثر لجلاء بعض المسائل التقنية أو الفنية فيعين النائب العام الخبير المختص ويحدد مهمته بدقة. إذا كانت حالة المجني عليه تستلزم المعاينة الطبية أو التشريح فيستدعي النائب العام الطبيب الشرعي أو الطبيب المختص ويكلفه بالمهمة المطلوب تنفيذها بدقة ووضوح. لا يباشر الخبير أو الطبيب مهمته إلا بعد ان يحلف اليمين بأن يقوم بها وفق ما يفرضه الضمير والشرف. لا يحق له ان يتجاوز المهمة المحددة له. بعد ان ينجزها يضع تقريرا يذكر فيه المرجع الذي عينه والمهمة المحددة له والإجراءات التي قام بها والنتيجة التي خلص إليها.

والخبير هنا يقصد به الشركات أو الاشخاص الذين لا تتعدى مهامهم تقديم المشورة التقنية العلمية.

وينص المرسوم الاشتراعي رقم ٥٤ الصادر في ١٧ آذار ١٩٥٧ على ان هناك جداولُ توضع كل ثلاث سنوات من قبل مجلس القضاء الأعلى يصدق عليها وزير العدل. [22]

الأمر الذي يشكل أهمية كبيرة في القضايا التي تكون الأدلة فيها مستخرجة من العالم الرقمي المعقد، وخاصةً مع غياب الاضطلاع الكافي للقضاة في هذا المجال. وبالتالي أحيطت الخبرة بقواعد شكلية تحفظ لها مكانتها إذ لتقرير الخبير قوة ثبوتية كبيرة خاضعة لتقدير القاضي على أن يكون معللًا بشكلٍ واضحٍ.

بالإضافة إلى ذلك فإن الاستفادة من أصحاب الاختصاص لا تقتصر فقط على تقديم التقارير أمام المحاكم بل يشمل أيضًا الخضوع بشكل مستمر لدورات تدريبية تجمع القضاة والضباط وعناصر الضابطة العدلية والخبراء التقنيين في العالم الرقمي من أجل رفع مستوى الإلمام بالعالم الرقمي والتعرف على التعابير التي تستخدم في هذا المجال، وتوحيد اللغة القانونية بينهم، ووضع نماذج موحدة في رفع الدليل الرقمي يتم اتباعها منذ لحظة بدء التحقيق الأولي مرورا بالتحقيق الابتدائي، وصولا إلى المحاكمة. إذ إن تقرير الخبير لا يلزم القاضي الجزائي الذي يحكم حسب قناعته الشخصية وهو الذي يقدر قيمة النتائج التي توصل إليها الخبير في تقريره، لذلك لا بُدّ من تكوين القاضي معرفة كافية تسمح له بذلك.

وعلى سبيل المثال، وإظهارًا لدور الخبراء التقنيين في مساعدة القضاة:

عام ٢٠٠٠، رفع اتحاد الطلبة إليهود في فرنس دعوى ضد شركة "YaHoo" الفرنسية والأميركية، بسبب وجود مزاد علني يتعلق بالنازية على إحدى الصفحات المجانية التي تبث من خلال الشركة

---

[22] نصر (فيلومين)،**أصول المحاكمات الجزائية، دراسة مقارنة و تحليل**، الطبعة الأولى ٢٠١٣ ،المؤسسة الحديثة للكتاب ص٤٧٢.

على الإنترنت. ولقد تضمن المزاد عرضًا لمجموعة من صور الزعيم " أدولف هتلر" ومجموعة شعارات وصور وأعلام تتعلق بالحزب النازي.[23]

وقد رفعت الدعوى أمام محكمة باريس الابتدائية، بناء على أن شركة "ياهو" خففت من فظائع كارثة "الهولوكوست" عندما سمحت بالمزاد على الإنترنت.

لقد أصدر القاضي حكمه على شركة "ياهو" الفرنسية بإلزامها بمنع المستخدمين من الدخول إلى هذه المزادات، واعتمد القاضي في حكمه على تقرير الخبرة التقنية الذي أكد قدرة الشركة على القيام بذلك. ولم يكن للقاضي أن يعلم بذلك لولا مساعدة الخبير التقني.[٢٤]

لقد استعرضنا في ما سبق أهمية تخصيص الأجهزة الأمنية مكاتب تتمتع بالاحترافية عالية في العمل والتعاطي مع الأدلة الرقمية والعالم السيبراني الواسع وعدم إغفال التنسيق والتعاون الدائم مع القطاع الخاص وأصحاب الخبرة التقنية العالية من أجل ضمان استمرارية التطور، تماشياً مع تطور العالم

---

[23] عبد الرؤوف الخنّ جريمة الاحتيال عبر الإنترنت، مرجع سابق، ص ٣٣٨.

[24] http://juriscom.net/wp-content/documents/yahoo20050517.

TGI Paris, référé, 22 mai 2000, UEJF et Licra c/ Yahoo! Inc. et Yahoo France : Juriscom.net:

Ainsi, le 22 mai 2000, le juge délégué par le premier président avait ordonné à Yahoo! Inc. de prendre toutes les mesures de nature à dissuader et à rendre impossible toute consultation sur "yahoo.com" du service de ventes aux enchères d'objets nazis et de tout autre site ou service qui constitue une apologie du nazisme ou une contestation des crimes nazis, **après avoir recueilli les avis des experts confirmant la possibilité d'effectuer sans coût prohibitif un filtrage efficace à environ 80%, le juge a confirmé cette ordonnance**.

الرقمي. ولكن ذلك لايكفي من دون مواكبة متوازية للقوانين التي ترعى إجراءات التفتيش والمصادرة التي تنفذها الضابطة العدلية في الجرائم العادية، وتطويرها، من أجل أن تشمل العالم الرقمي أيضًا، وهذا ما سنبحثه في الفصل القادم.

الفصل الثاني: رفع الدليل الرقمي في ضوء التشريع اللبناني

لقد حدد قانون أصول المحاكمات الجزائية اللبناني، المهام والإجراءات التي يجب على الضابطة العدلية القيام بها عند وقوع الجريمة، من حماية مسرح الجريمة والاستماع الى الشهود وتوقيف المشتبه فيهم إلى جمع الأدلة المتاحة كافة، في سبيل كشف الحقيقة. لن ندخل في هذا الفصل في جميع المهام الموكلة إليها أثناء التحقيق الأولي، بل سنتناول الشق المتعلق بجمع الأدلة والأشياء التي تساعد في معرفة مرتكبي الجرائم وإحقاق الحق والعدالة، وبالتحديد الأدلة الرقمية. فهل المواد القانونية في قانون.أ.م.ج المتعلقة بجمع الأدلة قادرة على مواكبة التطور المعلوماتي الرقمي، أم أننا في حاجةٍ إلى نصوصٍ جديدةٍ تواكب التطور التقني؟

لقد ميّز المشرّع اللبناني بين ما إذا كانت الجريمة مشهودة، حيث منح الضابط العدلي صلاحيات أوسع نسبياً من أجل تأمين السرعة في توقيف المشتبه بهم، وبين الجريمة غير المشهودة حيث نلاحظ بشكل واضح التشدد في تضييق صلاحية الضابطة العدلية، من أجل السيطرة على إجراءات التفتيش والمصادرة، وجمع الأدلة وضمان عدم حصول التجاوزات[25].

إلّا أنَّ الجريمة المتصَوَرة، حين وُضعت هذه المواد، هي الجريمة التقليدية أو العادية. والأدلة المقصودة فيها هي الأدلة المعروفة من الجميع (كالبصمات وأداة الجريمة وأي شيء ملموس ومحسوس يساعد في كشف الحقيقة) وبالتالي فهذه المواد ليست مهيَّئة لاستيعاب الأدلة الرقمية الحديثة الناتجة عن جرائم المعلوماتية او عن الجرائم العادية الأخرى وما يستتبع معها من تعقيدات ومشاكل قانونية وتقنية:

فالدليل الرقمي هو دليل غير ملموس، وهو من صنع الآلة، وقد يحتاج مهارات تقنية خاصة لجمعه، فالضابط العدلي أو المحقق ليس أمام مسرح جريمة واحد كمسرح جريمة القتل مثلاً، بل هو أمام مسرحين، مسرح ملموس يتمثل بالحاسوب أو الهاتف أو الجهاز بشكل عام، ومسرح آخر افتراضي لا

[25] Habib (Mohamed), **Le droit pénal libanais à l'épreuve de la cybercriminalité** ,Edition Juridique Sader ,1ère édition 2011,Beirut, Liban P 178

حدود له، ففي الأول عليه معرفة التعامل مع الآلة ونظام المعلومات المشغَّل فيها، وفي الثاني عليه التمتع بالمعرفة التقنية العالية من أجل ضمان سلامته وعدم المس بموثوقيته. هذا من جهة، ومن جهة أخرى فان إيجاد الدليل الرقمي هو خطوة أساسية ومهمة في التحقيق، إنما رفعه أو مصادرته إذا صح التعبير، والحفاظ عليه، فهو أمر في غاية الدقة ويحتاج إلى خبرة كبيرة في المجال لكونه عرضة للتشويه في أي وقت من مراحل التحقيق، وسنفصل هذا الموضوع لاحقاً.

ولا بُدّ من التمييز هنا بين الدليل الرقمي الذي يمكن رفعه من الآلة (حاسوب ، هاتف، الخ) كونه مخزن فيها وهو ما يعرف بالدليل الثابت، وبين الدليل الرقمي الديناميكي الذي قد يتم اعتراضه في العالم الرقمي أثناء حركة البيانات والمعلومات، وهذا ما يعرف باعتراض الاتصالات والمراقبة الإلكترونية. ومثالاً على ذلك فإن الحصول على فيديو مسجل على الحاسوب يختلف عن القدرة على الدخول إلى كاميرات المراقبة ومشاهدة ما يحدث في الوقت الحقيقي، ولكل من هاتين الحالتين معايير وقوانين مختلفة، سيما وأن الحالة الثانية قادرة بشكل واضح على خرق الحق في الحياة الخاصة والحرية الشخصية المنصوص عنه في المادة ١٢ من الإعلان العالمي لحقوق الإنسان[26].

تكثر الأسئلة والاشكاليات في هذا المجال لذلك سوف نحاول في هذا الفصل إلقاء الضوء على موقف المشرع اللبناني أمام تعقيد الدليل الرقمي والصعوبات التي تواجه القضاء والضابطة العدلية أثناء جمعه واستخراجه من الآلة أو من خلال اعتراضه أثناء انتقال حزمات المعلومات أو ما يسمى بالمراقبة الإلكترونية.

[26] **المادة ١٢ من الإعلان العالمي لحقوق الإنسان:** لا يتعرض أحد لتدخل تعسفي في حياته الخاصة وأسرته ومسكنه أو مراسلته أو لحملات على شرفه وسمعته ، و لكل شخص الحق في الحماية من مثل هذا التدخل أو تلك الحملات

المبحث الأول: الصعوبات التي تواجه إجراءات التفتيش

قبل البدء بتفصيل هذا المبحث لا بُدّ لنا من طرح إشكالية قانونية قد تواجه النيابة العامة والضابطة العدلية عند جمع الدليل الرقمي. جاء في المادة ٤١ أ.م.ج[27] (التي تتناول الإجراءات المتخذة عند اكتشاف الجريمة المشهودة) أن الضابط العدلي يقوم بالتحريات ويقبض على من تتوافر شبهات قوية حول ارتكابه الجريمة أو إسهامه فيها ويجري التفتيش في منزله ويضبط ما يعثر عليه من مواد جرمية أو أشياء ممنوعة.

وجاء في المادة ٤٣ أ.م.ج: "إذا رأى الضابط العدلي أن ثمة أوراقًا أو أشياء تفيد التحقيق موجودة[28] ......"

---

[27]– **المادة ٤١ أصول محاكمات جزائية:** إذا وقعت جريمة مشهودة ينتقل الضابط العدلي فورًا إلى مكان حصولها ويبلغ النائب العام المختص بها. ويحافظ على الآثار والمعالم والدلائل القابلة للزوال وعلى كل ما يساعد على جلاء الحقيقة. يضبط الأسلحة والمواد المستعملة في الجريمة أو الناتجة عنها. يستمع إلى الشهود دون تحليفهم اليمين. يقوم بالتحريات ويقبض على من تتوافر شبهات قوية حول ارتكابه الجريمة أو اسهامه فيها ويجري التفتيش في منزله ويضبط ما يعثر عليه من مواد جرمية أو أشياء ممنوعة. يستعين بالخبرة عند الاقتضاء. له أن يستجوب المشتبه فيه شرط ان يدلي بأقواله بإرادة واعية حرة ودون استعمال أي وجه من وجوه الإكراه ضده. إذا التزم الصمت فلا يجوز إكراهه على الكلام. على الضابط العدلي الذي يتولى التحقيق في الجريمة المشهودة أن يطلع النائب العام المختص على مجرياته وان يتقيد بتعليماته. إذا كلف النائب العام المختص الضابط العدلي ببعض الاعمال التي تدخل ضمن صلاحياته فعليه أن يتقيد بمضمون التكليف.

[28]– **المادة ٤٣ أصول محاكمات جزائية:** إذا رأى الضابط العدلي أن ثمة أوراق أو أشياء تفيد التحقيق موجودة لدى شخص لم تتوافر شبهات قوية ضده يكون للنائب العام أو لقاضي التحقيق، دون الضابط الآلي، أن يجري التفتيش في منزل هذا الشخص ما لم يوافق هذا الأخير دون إكراه على أن يقوم الضابط العدلي بالتفتيش. كل تفتيش تجريه الضابطة العدلية في أحد المنازل، خلافا للأصول التي حددها القانون للنائب العام في الجناية المشهودة، يكون باطلًا. يتعرض الضابط العدلي الذي يدخل المنزل, خلافا لهذه الأصول ويجري التفتيش فيه، للملاحقة بالجنحة المنصوص عليها في المادة ٣٧٥ من قانون العقوبات غير أن الإبطال في هذا الشأن يقتصر على المعاملة الباطلة ولا يتعداه إلى سائر إجراءات التحقيق.

والسؤال المطروح هنا، ماذا لو كانت الأشياء التي تفيد التحقيق بيانات وأدلة رقمية؟ هل يجوز شملها بكلمة شيء أو مواد؟ وماذا عن شمول إجراءات التفتيش تفتيش الوسط الافتراضي؟

١- الاتجاه الرافض[٢٩] :

ويرى أن المقصود بلفظ "الشيء" هو ما كان مادياً أي ملموسًا، ولذا فإن الوسط الافتراضي والبيانات غير المرئية أو الملموسة لا يمكن اعتبارها أشياءً، ومن ثم لا يطبق عليها النص القانوني الذي استعمل مصطلح "شيء"، ما يجعل تفتيش الوسط الافتراضي وضبط محتوياته مخالفاً للقانون، ولمواجهة هذا القصور التشريعي يقترح البعض رأيًا بأن يتم تعديل النصوص الخاصة بالتفتيش وذلك بأن يضاف إليها ما يجعل التفتيش يشمل البحث في الوسط الافتراضي، وضبط المواد المعالجة عن طريق الحاسب الآلي، أو بيانات الحاسب الآلي. وهذا ما فعله المشرع الفرنسي في المادة ٥٥-١-١[30] والمادة ٧٧-١-١[31] من أصول المحاكمات الجزائية المعدلة بالقانون رقم ٧٣١ حزيران٢٠١٦.

٢٩ الجملي(طارق)،الدليل الرقمي في مجال الإثبات الجزائي، مقال منشور على الموقع الالكتروني (last revision 23/12/2019) www.startimes.com

30 **Procédure pénale francais (mars 2004) alinea 56:** Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, **données informatiques** ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, informations ou objets relatifs aux faits incriminés.

31 **LOI n°2016-731 du 3 juin 2016 alinea 77-1-1** Le procureur de la République ou, sur autorisation de celui-ci, l'officier de police judiciaire, peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des informations intéressant l'enquête, y compris celles issues **d'un système informatique ou d'un traitement de données nominatives**, de lui remettre ces informations, notamment sous

الاتجاه المؤيد:

ويذهب إلى أن التفتيش والضبط لا يقتصران على الأشياء بمفهومها المادي، لأن الغاية من التفتيش هي البحث عن دليل بشأن جريمة وقعت، ولذا فإن إعمال قواعد التفسير المنطقي تجعل من الكيانات المنطقية أهدافًا يمكن تفتيشها وضبط ما فيها من محتويات .

ووصولًا إلى النتيجة ذاتها يرى البعض الآخر[32] أنه يجب أن نرجع إلى مدلول كلمة شيء في العلوم الطبيعية، حيث تعني كل ما يشغل حيزاً مادياً في فراغ معين. ولما كانت الكيانات المنطقية، والبرامج، تشغل حيزاً مادياً في ذاكرة الحاسب الآلي، ويمكن قياسها بمقياس معين، وهى أيضًا تأخذ شكل نبضات إلكترونية تمثل الرقمين صفر أو واحد، فإنها ذات كيان مادي، وبالتالي يمكن ضبطها، لذلك لا مبرر لإدخال تعديلات جديدة على النصوص التشريعية.

الّا أنّنا نرى، انه يجب ألا نقف عند تفسير لفظة "شيء" بالمعنى الحرفي للكلمة، إذ يجب تفسير النص تفسيراً منطقياً، فما عناه المشرع من إجازة التفتيش، يعني إتاحة الفرصة للبحث عن الدليل الذي يساعد في كشف الحقيقة بشأن جريمة وقعت، ولا شك في أن المشرع حينما استعمل كلمة "شيء"، لم يكن يقصد بهذه الكلمة مفهومها الحرفي، إذ إن ما قصده هو البحث عن الدليل في موضعه، بصرف النظر عما إذا كان موضع البحث شيئا مادياً أو معنوياً، وما إذا كانت الأشياء المراد ضبطها مادية أو معنوية. غاية ما في الأمر أن المشرع حين وضع النص، لم ترد في ذهنه مسألة الوسط الافتراضي لعدم شيوعه آنذاك. وهذا الأمر ليس بغريب ، فسرقة الطاقة لم تشكل جرمًا في قانون العقوبات اللبناني إذ إن المادة ٦٣٥ في قانون العقوبات قد عرّفت السرقة "بأنها أخذ مال الغير المنقول خفية أو عنوةً بقصد التملك" والكهرباء لم تعتبر من المال المنقول ما أدى إلى تعديل

---

forme **numérique**, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel

[32] الحسيني(عمار)، **التصوير المرئي والتسجيل الصوتي وحجيتهما في الإثبات الجزائي**، المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، طبعة اولى، سنة ٢٠١٧ ص٨٢

القانون في المرسوم الاشتراعي ١١٢ تاريخ ١٩٨٨/٩/١٦ بحيث اضيف الى المادة "تنزل الطاقات المحرزة منزلة الأشياء المنقولة في في النصوص الجزائية".

ولكن المشرع اللبناني حسم النقاش بإقراره القانون رقم ٨١ تاريخ ١٠-١٠-٢٠١٨ متناولاً فيه إمكانية اتباع إجراءات التحقيق كافة في الجريمة المشهودة وغير المشهودة، إذا كانت الجريمة إلكترونية أم عادية، إن كانت الأدلة رقمية أم تقليدية، نتوسع في الشرح في مستهل البحث.

إن هذه الإشكالية القانونية المطروحة ليست العقَبةَ الوحيدة التي تواجه إجراءات التفتيش للضابطة العدلية، بل وبسبب حداثة الدليل الرقمي، يظهر في سياق التحقيق العديد من الصعوبات والمشاكل التي قد تعيق عملية السرعة والمشروعية في جمع الدليل، وهذا ما قد يقف حاجزا أمام إحقاق الحق والعدالة.

البند الأول: تفتيش مكونات الآلة الموجودة في المنزل

تتكون عملية التفتيش عن الأدلة في مسرح الجريمة من إجراءات دقيقة وحساسة، وأي خلل قانوني ناتج عن خطأ ما في جمع الدليل قد يجعل منه غير صالح للنظر به، فكيف إذا كان الدليل دليلًا رقمياً موجودًا في عالم افتراضي غير ملموس. والعالم الافتراضي الذي نتحدث عنه قد يكون ذاكرة الآلة أو الفضاءَ السيبراني و الناتوورك. ولكل من هذين العالمين إجراءات مختلفة تقنياً نعرضها نظرًا لأهميتها:

نبدأ بالحالة التي يكون فيها الدليل الرقمي مخزنًا أو موجودًا داخل محتويات الآلة(حاسوب وهاتف) والحصول عليه يتم من خلال الدخول إلى الأجزاء المكونة لها، وليس عبر اعتراض حركة البيانات الإلكترونية أو مراقبتها.

وهنا لا بُدّ من التمييز بين أمرين أساسيين، الأول: رفع الدليل الرقمي المخزن في الآلة ذاتها الموجودة في المنزل أو المكان المراد تفتيشه. والثاني: التفتيش عن الدليل الرقمي المخزن في ذاكرة آلة أخرى موجودة في منزل آخر، إنما يمكن الوصول إليها من النظام المعلوماتي للآلة المراد تفتيشها

في الأساس أو من مكتب المحقق[33]. ولهذا الموضوع نواح تقنية صعبة ومتطورة وتحتاج إلّمامًا كبيرًا في عالم التكنولوجيا والبرامج الرقمية. وأي خلل في هذه الإجراءات قد تهدد سلامة الدليل ومصداقيته أمام القاضي.

عند دخول المنزل المراد تفتيشه (أكان ذلك في حالة الجريمة المشهودة أو غير المشهودة) يكون الضابط العدلي أمام حالتين مختلفتين، لكل منهما صعوبات خاصة بها: الحالة الأولى تكون فيها الآلة المراد تفتيشها تعمل بشكل طبيعي، والدخول إليها لا يحتاج كلمة سر محددة، وهي الحالة الأسهل، والحالة الثانية التي يكون فيها الجهاز مزودًا بمنظومة حماية أو كلمة سر للتمكن من الدخول إليه[34].

<u>الحالة الأولى : حالة الوصول السهل</u>

في فرنسا، ينص قانون أصول المحاكمات الجزائية بشكل صريح على إمكانية قيام الضابط العدلي بتفتيش النظام المعلوماتي(الحاسوب أو غيره) الموجود في المنزل وضبط المعلومات الرقمية المخزّنة فيه.[٣٥]

أما في لبنان فإن إجراءات تفتيش الجهاز الإلكتروني تكون خاضعة بشكل كلي للمواد ٤٢و٤٣و٤٧ من قانون أ.م.ج، التي سمحت للضابط العدلي اتخاذ الإجراءات اللّازمة والضرورية كافة، لضبط الأدلة وإجراء الدراسات العلمية والتقنية لكشف هوية مرتكب الجريمة.[36] أي أنها شملت في محتواها

---

[33]Chaer (Nidal),**La Criminalité informatique devant la justice pénale**,edition juridique sader 2004, Beirut, Liban page 247

[34] Habib (Mohamed), **Le droit pénal libanais à l'épreuve de la cybercriminalité** ,Edition Juridique Sader ,1ère édition 2011,Beirut, Liban p 172

[35] **Article 57-1**Modifié par Loi n°2016-731 du 3 juin 2016

[36] Habib, **Le droit pénal libanais à l'épreuve de la cybercriminalité** op.cit p:173

تفتيش الحواسيب والأجهزة في المنزل أو المكان المراد تفتيشه. وبالتالي فليس هناك من مشكلة في مثل هذه الحالة، أما الصعوبة فتكمن في الحالة الثانية:

الحالة الثانية :حالة وجود كلمة سر

إذا كان دخول الآلة وتفتيشها من دون كلمة سر أمرًا سهلًا ومشمولًا بالقانون الجزائي، فإن العكس، أي تزويد الآلة بمنظومة حماية يجعل من التفتيش أمراً يشوبه العديد من الصعوبات القانونية والتقنية. سوف نكتفي بدرس الصعوبات من الناحية القانونية ولن ندخل، في طبيعة الحال، في المتاهات التقنية كون تجاوز كلمة السر يحتاج إلى اخصائيين ومحترفين في مجال البرمجة.

لم يأتِ القانون الجزائي اللبناني في مواده، على ذكر وجوب الحصول على موافقة صاحب المنزل المراد تفتيشه من قِبَل النيابة العامة[37] الّا أنَّه لم يعط الصلاحية نفسها للضابطة العدلية: فعند وجود شبهات قوية ضد أحد الأشخاص لايعطى الأمر بتفتيش منزل المشتبه فيه، إلا بعد أن يُسمح بذلك، دون إكراه، صاحب المنزل.

اما النائب العام أو قاضي التحقيق فله أن يقوم بالتفتيش دون ضرورة الموافقة، وبالتالي فإن موافقة صاحب العلاقة مطلوبة فقط، عند قيام الضابط العدلي بالتفتيش دون النائب العام أو قاضي التحقيق على عكس القانون الفرنسي الذي ينص في المادة ٧٦ منه على ضرورة موافقة صاحب العلاقة في جميع الحالات ما خلا الجريمة المشهودة[38].

و بالتالي فإن صلاحيات الضابطة العدلية والمحققين، تصطدم بالحقوق الممنوحة للمشتبه بهم ومنها الحق بالدفاع، والحق بالحرية الشخصية. وما من شيء يجبر المشتبه فيه على التعاون مع الضابطة العدلية، والإدلاء بأي معلومات قد تدينه. رغم أن قانون أصول المحاكمات الجزائية اللبناني لم ينص

---

[37] قهوجي(علي)، شرح قانون أصول المحاكمات الجزائية، منشورات الحلبي الحقوقية بيروت لبنان ص ٦٩

[38] **Art 79 du code de procédure pénale français**: " les perquisitions visites domiciliaires et saisis de pièces ne peuvent êtres effectuées sans l'assentiment exprès de la personne chez qui l'opération a lieu.

بشكل واضح على ذلك بل يمكن استنتاجه من المادة ٤١ التي جاء فيها :" إذا التزم الصمت فلا يجوز إكراهه على الكلام "و من المادة ٤٧ في الفقرة الأولى : "إن امتنعوا أو التزموا الصمت فيشار إلى ذلك في المحضر ولا يحق لهم اكراههم على الكلام أو استجوابهم تحت طائلة بطلان إفادته".

من هنا يتبين لنا أن حق المشتبه فيه بالتزام الصمت يشكل عقبة حقيقية أثناء البحث عن الدليل الرقمي إذا قرر المشتبه فيه الامتناع عن إعطاء كلمة السر وأعاق الدخول الى بياناته وليس للضابطة العدلية أو النيابة العامة إرغامه على الكلام، وبالتالي لا بُدّ من الاستعانة بالخبرات التقنية والتكنولوجية للعمل على الدخول إلى مكونات الحاسوب ورفع الدليل الرقمي.

البند الثاني: الدخول عن بعد على حاسوب آخر في منزل آخر

سبق وذكرنا أنه في جريمة المعلوماتية هناك مسرحا جريمة، مسرح حسي ملموس متمثل بمكونات الآلة أو الحاسوب (Hardware)، ومسرح افتراضي وهو الفضاء السيبراني أو network. والمفارقة هنا أنه من خلال هذا الفضاء يمكن الولوج إلى كل الأجهزة والحواسيب الموصولة إليه.

تتم العملية من خلال دخول المستخدم عبر الجهاز(حاسوب أو هاتف...) إلى Network أو الإنترنت بحيث يصبح داخل هذا العالم الافتراضي، ومع المعرفة التقنية، والبرمجة الكافية، يمكن لهذا المستخدم الدخول إلى أي جهاز آخر موصول إلى الفضاء الرقمي أو Nertwork. وهذه التقنية يستخدمها العديد من المجرمين(القراصنة الرقميين) للدخول إلى الصفحات الخاصة للمستخدمين العاديين والحصول على معلوماتهم الخاصة ولابتزازهم أو التشهير بهم، وهذا نوع من أنواع جرائم المعلوماتية.

الّا أنَّ هذه الطريقة قد تستخدم أيضًا من قبل الضابطة العدلية أو القضاء من أجل الحصول على أدلة رقمية من جهاز آخر في مكان آخر داخل الأراضي الإقليمية بشكل سريع لضمان عدم ضياع الأدلة والوصول إلى الحقيقة بما أمكن من السرعة. وتقنية التحقيق هذه هي تقنية حديثة، وحداثتها تتطلب تجددًا وحداثة في المواد القانونية من أصول المحاكمات، لمنحِ الدليل الرقمي المشروعية والقوة الثبوتية أمام المحكمة، والحد من إمكانية رفضه، وهذا ما فعله المشرع الفرنسي.

فما هي الخيارات المتاحة أمام الضابط العدلي، عندما يجد أن دليلاً رقمياً موجودًا داخل ذاكرة حاسوب أو جهاز في منزل آخر؟ هل عليه الانتقال إلى هذا المكان بعد أخذ الإذن من المدعي العام؟ ماذا لو كان في الإمكان الحصول على هذا الدليل عن بعد، بواسطة الجهاز الموجود أمامه؟

١- **الانتقال إلى المكان الآخر**

إن الانتقال إلى المنزل الآخر أمر متاح في أي وقت، شرط الحصول على مذكرة تفتيش أخرى من قبل المدعي العام أو قاضي التحقيق أو بعد موافقة صاحب المنزل. عملًا بالنصوص القانونية، الاّ أنَّ ذلك لا يتناسب مع طبيعة الدليل الرقمي الذي قد يكون عرضة للزوال والتغيير خاصةً اذا تمكن المشتبه فيه الأول من التواصل مع المشتبه فيه الثاني المراد تفتيش منزله طالبًا منه مَحو الأدلة الرقمية نهائياً عن النظام المسجلة فيه المعلومات والبيانات.

٢- **الدخول عن بعد**

إن المشكلة التي تصادف الضابط العدلي هنا هي أنه في إطار القواعد التقليدية في أصول التحقيق، لا بدّ وأن تجرى عملية التفتيش بوجود صاحب المنزل[39] وهنا نعني أيضًا صاحب الجهاز المراد تفتيشه. وفي هذه الحالة يصعب تطبيق هذه القاعدة إذ إن الدخول إلى الجهاز يتم عن بعد. كما أن القانون يفرض على الضابط العدلي إعلام المشتبه فيه مسبقاً، واحترام القواعد التي تحمي حياته الخاصة وأن الدخول إلى ذاكرة جهازه والحصول على معلومات خاصة به من دون علمه أو موافقته ومن دون الدخول فعلياً إلى المنزل يشكل خرقاً للمادتين ٥٧١ و٥٧٢ من قانون العقوبات المتعلقتين بخرق حرمة المنزل.

---

[39] **المادة ٣٣ أ.م.ج:** للنائب العام أن يدخل إلى منزل المشتبه فيه للتفتيش عن المواد التي يقدر أن تساعد في إنارة التحقيق. وله أن يضبط ما يجده منها وينظم محضرًا بما ضبطه واصفًا إياه بدقة وتفصيل وأن يقرر حفظ المواد المضبوطة بحسب طبيعتها ويجري التفتيش بحضور المشتبه فيه أو المدعى عليه إن لم يكن حاضرًا أو تمنع عن الحضور أو كان متواريا عن الأنظار فيجري التفتيش بحضور وكيله أو إثنين من أفراد عائلته الراشدين أو شاهدين يختارهما النائب العام.

إن هذا النوع من التفتيش يتعارض مع مبدأ "مشروعية الدليل" الذي سوف نتناوله بالتفصيل في القسم الثاني من البحث، خاصةً وأنه لا يمكن البحث عن الحقيقة بأي وسيلة كانت، فإذا كانت هذه الوسيلة غيرَ مشروعة لا يمكن إثبات الحق في المحكمة.

و هنا يظهر اجتهاد فرنسي[40] ملفت يدعمه الفقه[41]، وهو رفض تشبيه صفحة الاستقبال الموجودة على الإنترنت الخاصة بالشخص، بمنزل وهمي خاص به.

ولكن المشرع الفرنسي، اتخذ إجراءات مناسبة من أجل تعديل إجراءات التفتيش في التحقيق الأولي مواكبةً للتطور التكنولوجي فتنصّ في المادتين ٥٧-١ [42] و٩٧-١ [43]على أنه يجوز للضابط العدلي أن يجري تفتيش الأجهزة في المكان المراد تفتيشه، والدخول إلى الشبكة المعلوماتية للحصول على معلومات وأدلة تفيد التحقيق، مخزنةٍ داخل النظام، أو في ذاكرة الآلة نفسِها أو في شبكة معلوماتية

---

[40] TGI PARIS (ordonnance de référé) 14 août 1996, jurisprudence p 490, note GAUTIER.

[41] Frayssinet **, internet et protection des données personnelles** , expertises 1998(avril)p 99

[42]Loi n°2016-731 du 3 juin 2016 - art. 58:

Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

[43]**Article 97-1**Créé par Loi 2003-239 2003-03-18 art. 17 3° JORF 19 mars 2003 L'officier de police judiciaire peut, pour les nécessités de l'exécution de la commission rogatoire, procéder aux opérations prévues par l'article 57-1.

أخرى طالما يمكن الوصول إليها. وطبعًا المقصود هنا تواجد الحواسيب والأجهزة داخل الأراضي الإقليمية وليس في الخارج، لأنه في مثل هذه الحالة، نصبح أمام مساعدة قانونية متبادلة بين الدول، وهذا موضوع القسم الأخير من بحثنا.

في لبنان، بقيت المواد القانونية التي ترعى إجراءات التفتيش والمصادرة حتى العام الماضي تقليدية، يشوبها العديد من الثغرات، كون المشرع اللبناني حين نص قانون أصول المحاكمات، لم يكن هناك وجود للعالم الرقمي كما هي الحال اليوم، وكانت الأدلة أدلة حسية ملموسة (بصمات، دماء، شعر،الخ..) ترفع من مسرح جريمة ملموس ومحدد جغرافياً، وليس في عالم فضائي افتراضي لا حدود له.

إلى ان أُعدت مجموعة نصوص قانونية متماسكة ومتكاملة، تغطي المسائل الأساسية الجديدة المتصلة بثورة تكنولوجيا المعلومات والاتصالات، وتنسجم في الوقت عينه مع النظام القانوني اللبناني، الذي ينتمي إلى النظام اللاتيني الجرماني، والمستوحى في معظم أحكامه من القانون الفرنسي. وجرى العمل على التوفيق بين الحاجات الناتجة عن التطور الإلكتروني وسلامة العمليات التجارية، بما يكمل ويصحح بعض الأحكام القانونية المرعية الإجراء، وبما يضيف عليها من أحكام جديدة قادرة على إدخال لبنان عالم الحداثة، وتلبية سرعة المعاملات التجارية، التي تحولت، بحكم التطور التكنولوجي، إلى عمليات إلكترونية سريعة لا تستقيم مع الإبقاء على الوسائل التقليدية التي تتضمنها التشريعات التي كانت نافذة.

الأمر الذي أدّى وبعد جهد جهيد، إلى إقرار قانون المعاملات الإلكترونية والبيانات الشخصية رقم ٨١ تاريخ ٢٠١٨/١٠/١٠ ولو متأخراً، وحددت في الفصل السابع فيه، القواعد الإجرائية المتعلقة

بضبط الأدلة المعلوماتية وحفظها، وتم تعريف الدليل الرقمي والآثار المعلوماتية التي تقوم الضابطة العدلية بإجراءات ضبطها وحفظها.[44]

وشدد على ضرورة توثيق الإجراءات والأعمال كافة المتعلقة بالدليل الرقمي من حيث الوصول إليه وسحبه ونسخه ثم نقله وحفظه، كل ذلك في سبيل الحفاظ على سلامته وموثوقيته أمام المرجع القضائي المختص.

و لقد جاء في الفقرة الأخيرة من المادة ١٢٣ في هذا القانون ما كانت تطالب به الضابطة العدلية من تأمين المشروعية لإجراءاتها في ضبط الأدلة المعلوماتية والبيانات على وسيطة إلكترونية مثل الأقراص المدمجة والحواسيب والهواتف والUSB ، بحيث تطبق أصول المحاكمات الجزائية المتعلقة بالتفتيش والمصادرة في الجريمة المشهودة وغير المشهودة، لا سيما المادتان ٣٣ و٤١ اللتان سبق وعرضنا مضمونها سابقاً.[45]

---

[44] **المادة ١٢١ قانون ٨١ تاريخ ١٠-١٠-٢٠١٨**: الآثار المعلوماتية, والتي هي من قبيل الأدلة الرقمية والمعلوماتية، هي البيانات التي يتركها الأشخاص بصورة إرادية أو لا ارادية على الانظمة وقواعد البيانات والخدمات المعلوماتية والشبكات المعلوماتية.

تتضمن الأدلة المعلوماتية: التجهيزات المعلوماتية والبرامج والبيانات والتطبيقات والآثار المعلوماتية وما يماثلها.
تتبع القواعد الواردة في هذا الفصل عند ضبط الأدلة المعلوماتية بناءً على قرار من النيابة العامة أو المرجع القضائي المختص.

يجب احترام الخصوصية لجهة الآثار المعلوماتية ولا سيما البيانات والصور غير المتعلقة بالدعوى الجزائية .

تقوم الضابطة العدلية بإجراءات ضبط الأدلة المعلوماتية وحفظها والمنصوص عنها في هذا الفصل, بناءً لقرار المرجع القضائي المختص. يؤازر الضابطة العدلية في ضبط الأدلة المعلوماتية وحفظها مكتب متخصص.

[45] **المادة ١٢٣ في القانون ٨١**: يجب ان ينظم محضر بكل عملية ضبط، أو حفظ، أو تحليل أو فحص او نقل او غيرها من مرجع إلى آخر لأي دليل معلوماتي او رقمي, على أن يتضمن عرضًا تفصيليًا لكل الإجراءات والاعمال المُجراة و المراجع كافة التي كان الدليل بحوزتها وكيفية نقله, لا سيما تلك التي تضمن سلامة الدليل وعدم إجراء أي تعديل عليه منذ لحظة ضبطه.

ولوضع حد للنقاش المتعلق بما إذا كان يمكن الدخول عن بعد من خلال حاسوب أو هاتف مراد تفتيشه أم يجب الحصول على إشارة جديدة من المرجع القضائي المختص، تحدّد المادة ١٢٤ انه يمكن ربط اي بيانات وأدلة رقمية موجودة في نظام معلوماتي داخل الأراضي اللبنانية إذا كان ممكنًا الوصول إليها من الجهاز المقرر تفتيشه.

ولقد كان هذا النص موفّقاً في إصابته للجدلية القائمة أثناء التحقيقات وضبط الأدلة الرقمية فيها، رغم أننا نرى أنه كان لا بُدّ من توضيح كيفية تنفيذ التفتيش للنظام المعلوماتي: هل يجب الانتقال حكماً إلى المكان الجغرافي أي المكان حيث يوجد فيه هذا النظام ليصار إلى تفتيشه أو يمكن إجراء ذلك من المكاتب الخاصة للضابطة العدلية من دون الانتقال؟ إن القانون رقم ٨١ لا يحدد بشكل صريح ما إذا كان يجب الانتقال إلى مكان وجود النظام المعلوماتي، ولكن يفهم من المادة ١٢٤ في القانون رقم ٨١ أنه لا داعٍ للانتقال توخيًا للسرعة رغم استخدام تعابير **ضبط وحفظ ونقل وإيداع**. والإشارة إلى ضرورة ختم المكان حيث تتم العملية أو النظام الإلكتروني بالشمع الأحمر الى حين وصول الشخص المتخصص [46].

في جميع الأحوال، يجب الاحتفاظ بنسخة مطابقة للأصل(عن البيانات و البرامج) كما ضُبطت عن الدليل الرقمي, ويتم وضع الأختام على الوسيطة الإلكترونية المحفوظة عليها, وإيداعها المرجع القضائي الذي قرر الإجراء مع المحاضر المنظمة.

مع مراعاة الأحكام الواردة في هذا الفصل, تطبق على ضبط الأدلة المعلوماتية أو البيانات على وسائط إلكترونية قابلة للنقل, مثل الأقراص المدمجة أو جهاز حاسوب, أحكام قانون أصول المحاكمات الجزائية المتعلقة بالتفتيش وضبط الأدلة الجريمة المشهودة وغير المشهودة, لا سيما المادتان ٣٣ و٤١ منه.

[46] **المادة ١٢٤ من القانون رقم ٨١** : ...... يمكن ضبط أية بيانات أو دليل رقمي مخزّن في نظام معلوماتي موجود على الأراضي اللبنانية إذا كان ممكناً الوصول إليها من النظام المعلوماتي المقرر تفتيشه.
يمكن الوصول إلى اية بيانات مخزنة في نظام معلوماتي، وضبطها، اياً كان مكان وجودها داخل او خارج لبنان، إذا كانت موضوعة بتصرف الجمهور أو في حال موافقة الشخص المخول قانوناً بإفشاء هذه البيانات من خلال نظام معلوماتي موجود على الأراضي اللبنانية. عند ضبط الدليل المعلوماتي , يمكن للنيابة العامة أو المرجع القضائي الناظر في الدعوى أن يقرر أن عملية تنزيل البيانات والبرامج أو نقلها أو نسخها يتم بحضور الشخص المعني، أو

مع العلم أنه في معظم الحالات يتم الحصول على الأدلة الإلكترونية بواسطة الانتقال إلى المكان وذلك لصعوبة القيام بخرق النظام المعلوماتي عن بعد من قبل الضابطة العدلية وما يحتاج ذلك من خبرة تقنية عالية المستوى من ناحية، ونظرًا إلى خطورة هذا الأمر، وعدم القدرة على مراقبة تصرفات الضابطة العدلية التي قد تتعسف في استخدام السلطة الممنوحة لها من القضاء.

وهنا يطرح السؤال التالي:

ماذا لو كان الدليل موجودًا في نظام معلوماتي خارج الأراضي اللبنانية فهل يمكن ضبطه من خلال الولوج إلى نظام معلوماتي في الأراضي اللبنانية؟

يحتاج هذا السؤال إلى دراسة ومناقشة واسعتين نبحثهما في القسم الثاني تحت عنوان:" التعاون الدولي أساس لجمع الدليل الرقمي". ولكن وبشكل سريع نقول: إن ذلك مرتبط بنوع المعلومات المراد الحصول عليها، فإذا كانت موضوعة أصلاً بتصرف الجمهور، فلا مانع من ذلك، وإذا وافق الشخص المخول قانوناً بإفشاء المعلومات فأيضًا لا مانع من ذلك، أما في الحالات الأخرى فلا بد من التعاون الدولي الواضح والفعال وضمن إطار الاتفاقيات الدولية الموقعة.

إن عملية ضبط البيانات الإلكترونية المخزنة داخل مكونات الآلة أو النظام الرقمي(الأدلة الرقمية)، في غاية الدقة والتعقيد وتحتاج إلى إطار قانوني، تقني، وإجرائي من أجل ضمان سلامتها ومصداقيتها أمام القضاء مع ما يرافق ذلك من حاجة إلى تدريب كبير ومتواصل لضباط وعناصر الضابطة العدلية و القضاء.

بحضور شخص فني متخصص بالمعلوماتية، يعينه هذا الشخص بموجب تفويض خطي .وعند الاقتضاء , يختم المكان حيث تتم العملية او الوسيطة الإلكترونية حيث توجد البيانات والبرامج, بالشمع الأحمر الى حين حضور هذا الشخص الفني ضمن المهلة المحددة , وإلا تتم العملية بحضور شخصين من أقارب الشخص المعني او وكيله او شاهدين , أو يصرف النظر عن حضورهم وفق ما يقرر المرجع القضائي المختص.

الّا أنَّه هناك طريقة أخرى في الحصول على الأدلة الرقمية لا تحتاج إلى دخول المنازل والتفتيش الكلاسيكي وهي غالباً ما تستخدم في رفع الأدلة الرقمية الديناميكية عبر اعتراض حزمات المعلومات المنقولة بين الشبكات والتي لا تكون مسجلة داخل مكونات الآلة بشكل ثابت وهو ما يعرف بالمراقبة الإلكترونية أو اعتراض الاتصالات الرقمية.

وإذا اعتبرنا أن ضبط الأدلة المسجلة أمر صعب، فالمراقبة الإلكترونية أمر أصعب وأكثر تعقيداً من الناحية القانونية والتقنية؛ ويترافق مع وجوب فرض قيود وضوابط للسيطرة عليه، لضمان عدم التحول إلى أنظمة بوليسية قمعية لا مكان للخصوصية الفردية فيها، وذلك لا يتم إلا من خلال قوانين متطورة واضحة وصارمة.

كيف عالج القانون اللبناني هذا الموضوع؟ ما هي الحالات التي تستوجب مراقبة الاتصالات الرقمية أو العادية، ومن هم الاشخاص المعنيون ومن هي السلطة التي تصدر القرار للاعتراض؟ ما هي الضوابط التي فرضها القانون اللبناني وكيف يضمن حماية البيانات الشخصية والخصوصية؟

أسئلة توضح الإجابة عنها حيزًا عريضًا من القضايا التي تتناولها المراحل اللاحقة من البحث.

<u>المبحث الثاني</u> اعتراض الاتصالات والمراقبة الإلكترونية

في اعتراض الاتصالات ومراقبة حركة البيانات والمعلومات بين الأفراد، قد يذهب البعض إلى التفكير في الأنظمة القمعية والشمولية التي تقوم على التجسس وجمع المعلومات والتي لا تعطي للفرد المساحة الخاصة للتعبير عن رأيه ومواقفه، الّا أنَّ هذه الطريقة في جمع المعلومات تَتَّبعها جميع الدول بما فيها الدول الرائدة في الأنظمة الديمقراطية، وفي مجال حقوق الإنسان واحترام الحياة الخاصة، وذلك نظرًا لأهميتها في الوقاية من الجرائم قبل حدوثها بكشف الشبكات الإجرامية النائمة من جهة، ومن جهة أخرى بالحصول على الأدلة الرقمية الواضحة غير المخزنة في ذاكرة الآلة اكان حاسوبًا أم هاتفًا والتي لا يمكن الحصول عليها باعتماد إجراءات التفتيش التي سبق وتحدثنا عنها في المبحث الأول، أي الأدلة التي لا يمكن الوصول إليها إلا عبر اعتراض حزمات المعلومات والبيانات الرقمية المرسلة في شبكة الإنترنت في الوقت الحقيقي.

التفتيش عن الأدلة الرقمية والمراقبة الإلكترونية يخضعان لقواعد مختلفة تماماً رغم أن العالم الرقمي يجمع بينهما:

<u>أولًا:</u> : إن التفتيش عن الأدلة الرقمية داخل ذاكرة الآلة في مكان معين، هو إجراء واضح تقوم به الضابطة العدلية بعد أخذ إشارة النائب العام، أو بطلب من قاضي التحقيق، ويتم ذلك في حضور المشتبه فيه وبعلمه على الأقل كما ذكرنا سابقًا. أما اعتراض الاتصالات أكان هاتفياً أم ألكترونياً، بواسطة الإنترنت أو الناتورك، فهو ذو طابع خفي وسري غير مرئي، كون المعلومات المراد اعتراضها ليست مخزنة في ذاكرة الآلة[47].

---

[47] Chaer (Nidal),**La Criminalité informatique devant la justice pénale**, op.cit p:250

ثانيًا: إن عملية اعتراض المكالمات والاتصالات الإلكترونية هي عملية مستمرة ولفترة زمنية معينة وتحتاج إلى مثابرة وجهد بشري، وكما سنشرح لاحقًا في هذا المبحث. أما التفتيش وضبط الأدلة فهو إجراء آني ثابت ولا يحتاج إلى مدة زمنية طويلة وينتهي عند جمع الأدلة المتوفرة [48].

الجدير ذكره أنه لا يمكن اعتبار التنصت على المكالمات وهو نفسه عملية المراقبة الإلكترونية فهذا أمر خاطئ:

نظام الاتصالات الهاتفية يقوم على إرسال الصوت فقط من هاتف ثابت أو محمول إلى هاتف آخر عبر شبكة من الكابلات والموجات ما دون الحمراء، وقد تم إنشاؤه قبل ظهور وسائل الاتصال الحديثة "الإنترنت" وINTRANET اللتين تعتمدان بروتوكول الإنترنت (IP ADRESS) وإرسال الصوت والصورة عبر هذا البروتوكول (VOICE OVER IP) مثل التطبيقات التي نستخدمها يوميًا الواتساب(WHATSUP) والسكايب (SKYPE) والسناب تشات...(SNAPCHAT) والانستاغرام (INSTAGRAM). فالتنصت على المكالمات أمر سهل تقنياً إذا قارناه بالاعتراض الإلكتروني الذي يحتاج تقنيات حديثة جداً ومعقدة، غالبًا ما تكون مستخدمة فقط في الدول المتطورة ونعطي مثالًا: الاستخبارات البريطانية (MI6)التي طورت أكبر نظام مراقبة واعتراض ألكتروني ECHELON[49]. والولايات المتحدة الأميركية التي استخدمت فيها وكالة مكافحة المخدرات سنة ١٩٩٥ برنامج "COMPUSERVE" لاعتراض البريد الإلكتروني للعديد من تجار المخدرات و مبيضي الأموال[50].

---

[48] المرجع السابق ص ٢٥١

[49] ECHELON : هو برنامج مراقبة (شبكة إشارات / شبكة تحليل وتحليل) تديرها الولايات المتحدة بمساعدة أربع دول أخرى موقعة على اتفاقية UKUSA الأمنية: أستراليا وكندا ونيوزيلندا ، والمملكة المتحدة.

بحلول نهاية القرن العشرين ، تطور النظام الذي يشار إليه باسم "ECHELON" إلى أبعد من أصوله العسكرية والدبلوماسية ليصبح "نظامًا عالميًا لاعتراض الاتصالات الخاصة والتجارية" (المراقبة الجماعية والتجسس الصناعي)

[50] Chaer (Nidal),**La Criminalité informatique devant la justice pénale** op.cit page 252

و لنتمكن من التمييز بينهما على الصعيد القانوني لا بُدّ لنا من التركيز بشكل سريع ومقتضب على الناحية التقنية:

بالنسبة للاتصالات الهاتفية الكلاسيكية، وبمجرد أن يطلب المشترك رقمًا يود مخابرته، تُبقى الشبكة الهاتفية اتصالاً مستمراً يبقى حيوياً إلى حين إقفال الخط، وبالتالي اعتراض هذه المكالمة يقتضي سحب خط رديف سلكي أو لاسلكي والاستماع إلى المخابرة.

أما في الاتصال الإلكتروني ، فالمعلومات لا تنقل بواسطة خط اتصال واضح بل بواسطة حزمات معلومات تنتقل عبر وصلات لاسلكية وسلكية بقيادة بروتوكولين: الأول هو للتحكم في نقل الحزمات TCP، والثاني بروتوكول الإنترنت IP[51] لذلك أثناء الاتصال تسلك حزمات المعلومات عدة مسالك بين الوصلات في شبكة الإنترنت إذ إن كل حزمة معلومات تسلك طريقها الخاص ضمن صف انتظار على المسلك الذي اتبعته، لذلك في اعتراض المخابرات عبر الإنترنت تحتاج إلى آلية تقنية أخرى قادرة على الوصول إلى المعلومات في وقت الإرسال الحقيقي.

والمعلومات التي نتحدث عنها هنا، هي عبارة عن نوعين لا بُدّ من التمييز بينهما نظرًا لقدرتها على التأثير، وخرق الخصوصية الفردية المحمية بدساتير البلاد: النوع الأول، هو المعلومات المتعلقة بحركة البيانات Données relatives au traffic من الآلة المرسِلة إلى الآلة المرسَل إليها (آلة: قد تكون هاتفًا أو حاسوبًا) أو ما يعرف في نظام الاتصالات ب "داتا المعلومات" و هي تشمل: رقم الخط الخلوي – صاحب الخط – الرقم التسلسلي للهاتف والهاتف الآخر – نوع الاتصال رسالة نصية، صوت – تاريخ ووقت ومدة الاتصال – رقم المتصل والمتصَل به –إسم المحطة المرتبط بها الرقم أثناء الاتصال –إسم المحطة المرتبط بها الرقم الآخر– الرقم التسلسلي للهاتف الرقم الآخر.

والنوع الثاني هو المعلومات المتعلقة بالمحتوى Données relatives au contenu ، أي مضمون الاتصال الهاتفي والإلكتروني. وهذا النوع هو الأخطر على الخصوصية الفردية، إذ إنه

---

[51] عيسى(ميشال)، التنظيم القانوني لشبكة الإنترنت، دراسة مقارنة في ضوء القوانين الوضعية والإتفاقيات الدولية،الطبعة الأولى ٢٠٠١، المنشورات الحقوقية صادر ص ٤٤

يحتوي على معلومات قد تكون خاصة جدًا بين المتصلين، وهو يحتاج إلى إجراءات كثيرة فيها صعوبة ودقة للتمكّن من الحصول على حركة البيانات.

إذا فالمراقبة الإلكترونية قد تشمل الحصول على حركة المعلومات في الوقت الحقيقي أو على محتوى الاتصالات وهي تختلف عن عملية التنصت على المخابرات الهاتفية الكلاسيكية.

وهنا يتجه الأمن العالمي إلى الاستثمار والتطوير في هذا المجال، من أجل زيادة القدرة على كشف جميع أنواع الجرائم وحتى تفادي حصولها، ولكن مع الحفاظ على هامش من الخصوصية الفردية، عبر وضع ضوابط تضمن عدم جنوح السلطتين التنفيذية والقضائية نحو الأنظمة الشمولية وقمع الحريات.

كيف تناول المشرع اللبناني موضوع المراقبة الإلكترونية؟ و إلى اي مدى يستطيع حماية الخصوصية الفردية امام التطور التقني الحاصل؟

البند الأول: المراقبة الإلكترونية في لبنان والقانون ١٤٠

لبنان أول بلد عربي أدخل إطاراً قانونياً لاعتراض الاتصالات وسمح للضابطة العدلية استخدام مراقبة الاتصالات والمخابرات من خلال القانون ١٤٠ الذي صدر عام ١٩٩٩، من أجل البحث عن الأدلة في الجرائم التي قد ترتكب أو ارتكبت. ولكنه في المقابل فرض شروطًا معينة ورقابة مشددة على آلية تطبيقها، لضمان عدم التعسف في استخدامها، والحفاظ على ميزة لبنان بنظامه الذي يكفل الديمقراطية والخصوصية الفردية.

لقد أجاز القانون في المادة الأولى منه مراقبة الاتصالات السلكية واللاسلكية (الهواتف الثابتة، الخلوية – الفاكس – البريد الإلكتروني ...)[52]، ولكن ليس بشكل مطلقٍ بل تبعًا لحالات محددة، إما من قبل القضاء، بحيث يكون قرار التنصت قضائيًا وإما من قبل السلطة التنفيذية فيكون القرار إداريًا.

١ – إجازة التنصت أو اعتراض الاتصالات بناءً لقرار قضائي

لقاضي التحقيق الأول في كل محافظة، أن يصدر عفواً أو بناءً على طلب من القاضي المكلف بالتحقيق قراراً باعتراض مكالمات المشتبه فيهم في الجرائم التي يعاقب عليها القانون لمدة لا تقل عن سنة واحدة وفي حالات الضرورة القصوى .[53]

مع العلم بأن مدّة السنة المنصوص عنها هي مدة قصيرة، فالجرائم التي تستحق هذه العقوبة لا يمكن، أن تكون من الجرائم الهامة وفي ذلك إعطاء هامش واسع جداً للقضاء بمراقبة واعتراض الاتصالات في جميع الجرائم، ما يتعارض مع الشرط الثاني الذي فرضه القانون وهو الحالة القصوى. وتختلف هذه العقوبة بين الدول ففي فرنسا مثلًا على الجرم أن يكون معاقبًا بسنتي حبس على الأقل[٥٤].

---

[52] **المادة الأولى في القانون ١٤٠** :الحق في سرية التخابر الجاري داخليًا وخارجيًا بأي وسيلة من وسائل الاتصال السلكية أو اللاسلكية (الأجهزة الهاتفية الثابتة، والأجهزة المنقولة بجميع أنواعها بما فيها الخلوي، والفاكس، والبريد الإلكتروني...) مصون وفي حمى القانون ولا يخضع لأي نوع من أنواع التنصت والمراقبة أو الاعتراض أو الإفشاء إلاّ في الحالات التي ينص عليها هذا القانون بواسطة الوسائل التي يحددها ويحدد أصولها.

[53] **المادة الثانية من القانون ١٤٠** :في حالات الضرورة القصوى, لقاضي التحقيق الأول في كل محافظة إما عفوًا أو بناء لطلب خطي من القاضي المكلف بالتحقيق, أن يقرر اعتراض المخابرات التي تجري بواسطة أي من وسائل الاتصال المبينة في المادة الأولى من هذا القانون, وذلك في كل ملاحقة بجرم يعاقب عليه بالحرمان من الحرية لمدة لا تقل عن سنة. يكون القرار خطيًا ومعللًا, ولا يقبل أي طريق من طرق الطعن.

[54] **Loi n"91-646 du 10 juillet 1991,JO du 13 juillet 1991** relative au secret des correspondances émises par la voie des communications électroniques.

هذا من ناحية أما من ناحية أخرى، فان تعبير "حالات الضرورة القصوى" يشوبها الكثير من الغموض، فكيف يتم التمييز بين حالات اعتبارها حالات قصوى ومن الذي يحدد هذه الحالات ؟ هل ذلك متروك للقاضي وحده؟

فالقانون ١٤٠ لا يجيب على هذا السؤال وبالتالي فإن التوسع في تفسير هذا التعبير قد يؤدي إلى نتائج خطيرة على الحياة الخاصة والخصوصية التي نفصّلها في المبحث الثاني. مع العلم ان المشرع قد تنبه إلى الموضوع في اعتراض الاتصالات بناءً على قرار إداري بحيث حصر الموضوع بالإرهاب والجريمة المنظمة والجرائم المخلة بأمن الدولة. [55]

<u>٢ – اعتراض الاتصالات بناءً لقرار إداري</u>

جاء في المادة التاسعة من القانون المذكور، أنه يحق لكل من وزير الدفاع الوطني ووزير الداخلية بعد موافقة مجلس الوزراء أن يسمحا باعتراض المخابرات من أجل جمع المعلومات في مكافحة الإرهاب والجرائم المنظمة وجرائم الاعتداء على أمن الدولة.[56]

وبالتالي نرى أن هذه المادة قد سمحت للسلطة التنفيذية اعتراض المكالمات من دون العودة إلى القضاء وهذا أمر في غاية الدقة والخطورة بحيث يعطي سلطة استثنائية تسمح للنواب والوزراء، مع ما يعني ذلك في لبنان وفي ظل المحيط العربي المجاور، بالعمل على اعتراض اتصالات المواطنين تحت غطاء الحفاظ على أمن الدولة، "بالمعنى الواسع جداً له".

---

[55] Habib, **Le droit pénal libanais à l'épreuve de la cybercriminalité**,op.cit p:189.

[56] **المادة ٩ من القانون ١٤٠:** لكل من وزير الدفاع الوطني ووزير الداخلية أن يجيز اعتراض المخابرات بموجب قرار خطي معلل وبعد موافقة رئيس مجلس الوزراء، وذلك في سبيل جمع معلومات ترمي إلى مكافحة الارهاب، والجرائم الواقعة على أمن الدولة، والجرائم المنظمة. يحدد القرار وسيلة الاتصال موضوع الإجراء، والمعلومات التي يقتضي ضبطها، والمدة التي تتم خلالها عملية الاعتراض، على أن لا تتجاوز هذه المدة الشهرين، وعلى أن لا تكون قابلة للتمديد إلا وفق الأصول والشروط عينها.

والدليل على ذلك أنه تمت محاولة فرض المادة ١٥ في هذا القانون التي كانت تمنع اعتراض المخابرات التي يجريها النواب والوزراء متذرعين، بالحصانة النيابية والوزارية، لولا تصدي المجلس الدستوري لها في القرار الذي أصدره في ١٩٩٩\١١\٢٤، بعد استدعاء قدمه عدد من النواب[57]؛ بحيث أبطل المادة ١٥ كلياً واعتبر أن التمييز بين رئيس مجلس النواب ورئيس مجلس الوزراء والنواب والوزراء عن بقية المواطنين أمر غير مبرر تجاه قانون التنصت، لا بمصلحة عامة، لا بنص دستوري (مواد الحصانة النيابية والوزارية) إذ إن التنصت يهدف إلى جمع الأدلة والمعلومات والإثباتات تمهيدًا للملاحقة الجزائية وبالتالي فهو غير خاضع لمواد الحصانة النيابية والوزارية.

ولقد أدى هذا القرار إلى تعديل المادة ١٥ في القانون رقم ١٨٥ الصادر في ٢٠٠٠\١٢\٢٧ بحيث أصبحت:" لا يجوز اعتراض المخابرات التي يجريها الرؤساء و النواب و الوزراء بموجب قرار إداري فقط وذلك تطبيقاً لمبدأ فصل السلطات وضمان عدم تدخل السلطة التنفيذية بالسلطة التشريعية.

ولكن ماذا عن رئيس الجمهورية ؟

بما أن الأمر يختلف في ما يتعلق برئيس الجمهورية لأنه مشمول بأحكام المادة ٦٠ من الدستور التي تجعله من جهة غير مسوؤل عند قيامه بوظيفته إلا عند خرقه الدستور أو في حالة الخيانة العظمى وأن اتهامه في هاتين الحالتين أو في ما خص الجرائم العادية لا يمكن أن يصدر إلا من قبل مجلس النواب بموجب قرار يصدره بغالبية الثلثين من مجموع أعضائه وهو يحاكم من أجلها أمام المجلس الأعلى لمحاكمة الرؤساء المنصوص عنه في المادة ٨٠ من الدستور وبالتالي فلا يمكن أن يكون محل ملاحقة جزائية من قبل النيابة العامة وقضاء التحقيق، وبالتالي لا يجوز بأي شكل من الأشكال أن تخضع مخابراته للتنصت والاعتراض، الأمر الذي لا ينطبق على رئيس مجلس النواب

---

[57] حسين الحسيني – عمر كرامي – قبلان عيسى الخوري – نايلة معوض – زاهر الخطيب – ايلي سكاف – نجاح واكيم –جبران طوق – بيار دكاش – طلال ارسلان

والنواب الخاضعين لأحكام المادتين ٣٩ و٤٠ من الدستور، لا على رئيس مجلس الوزراء والوزراء الذين ترعى أوضاعهم المادة ٧٠ من الدستور اللبناني[58].

و لقد انشأ القانون ١٤٠ **هيئة مستقلة** من الرئيس الأول لمحكمة التمييز ورئيس مجلس شورى الدولة ونائبين يسميهم رئيس مجلس النواب، وأناط بهذه الهيئة التثبت من قانونية الإجراءات المتعلقة باعتراض المخابرات المتخذة بناء على قرار إداري وأولتها صلاحيات واسعة لإجراء التحقيقات اللّازمة مع الأجهزة الأمنية والإدارية والفنية ومع مؤسسات القطاع الخاص المعنية في موضوع وسائل الاتصال والاستعانة بمن تشاء من أهل الخبرة.

و لكن المجلس الدستوري في القرار نفسه أبطَل أيضًا هذه المادة لأنه يعتبر ذلك تدخلاً من النائب في أعمال السلطة التنفيذية خاصةً وانه يقوم بإجراء تحقيقات مع أجهزة أمنية وإدارية، ما يعتبر خارج الحدود التي عينها الدستور في رقابته على أداء الحكومة وتشكيله اللجان البرلمانية للتحقيق وفقا للنظام الداخلي للبرلمان.

وعليه أُدخل التعديل في القانون ١٥٨ الذي سبق وذكرناه وأصبحت هذه الهيئة مشكّلة من الرئيس الأول لمحكمة التمييز ورئيس مجلس شورى الدولة ورئيس ديوان المحاسبة فقط.[59]

---

[58] **المادة ٧٠ المعدلة بالقانون الدستوري الصادر في ٢١/٩/١٩٩٠** لمجلس النواب أن يتهم رئيس مجلس الوزراء والوزراء بارتكابهم الخيانة العظمى أو بإخلالهم بالواجبات المترتبة عليهم ولا يجوز أن يصدر قرار الاتهام إلا بغالبية الثلثين من مجموع أعضاء المجلس. ويحدد قانون خاص شروط مسؤولية رئيس مجلس الوزراء والوزراء الحقوقية.

[59] المادة ١٦ من القانون ١٤٠ المعدلة :تنشأ هيئة مستقلة من الرئيس الأول لمحكمة التمييز ورئيس مجلس شورى الدولة ورئيس ديوان المحاسبة تناط بها صلاحية التثبت من قانونية الإجراءات المتعلقة باعتراض المخابرات المتخذة بناء على قرار إداري. ويترأس الهيئة القاضي الأعلى درجة.

تبلغ الهيئة قرارات اعتراض المخابرات المتخذة بموجب قرار إداري خلال ثمانية وأربعين ساعة من صدورها.

يعود للهيئة، خلال مهلة سبعة أيام من تاريخ التبليغ, النظر في قانونية الاعتراض وعند الضرورة إبلاغ رايها بشأنه إلى كل من رئيس مجلس الوزراء والوزير المختص. ويعود لها النظر في قانونية الاعتراض بناء على مراجعة كل ذي

بعد البحث في هذا القانون، لا بُدّ من القول إنه أضفى المزيد من التنظيم القانوني على الاتصالات في لبنان وكان لا بُدّ منه لضمان عدم حصول التجاوزات والاعتداء على خصوصية المواطنين ولكن لا يزال ينقصه العديد من النقاط، خاصةً وأنه منذ عام ٢٠٠٠ حتى الآن حصل تطور سريع وكبير في عالم الاتصالات:

أولاً: حصر القانون مَهمّة التنصت بوزارة الداخلية (القوى الأمنية) ولم يعطِ وزارة الاتصالات أي دور وهذا ما أدى في فترة من الفترات إلى الصدام بين شعبة المعلومات في قوى الأمن الداخلي ووزير الاتصالات على خلفية من المسؤول عن غرفة التنصت الموجودة في مبنى تابع لوزارة الاتصالات في "بيروت".

ثانيًا: يبدو بشكل واضح أن القانون رقم ١٤٠ رغم تعديله بالقانون رقم ١٥٨ لسنة ٢٠٠٠ تناول فقط موضوع اعتراض المخابرات الهاتفية والتنصت ولم يتناول المراقبة الإلكترونية، ولقد سبق وفصلنا الفرق بينهما، ورغم أنه ذكر في وسائل الاتصال البريد الإلكتروني.

قد يكون مردّ ذلك عدم إلمام المشرِّع اللبناني بالفرق التقني بين الاثنين. فعندما يذكر في المادة الأولى الهاتف الخلوي والهاتف اللاسلكي والفاكس فمن الواضح أنه كان يقصد الاتصال العادي وليس الاتصال عبر بروتوكول الإنترنت (TCP/IP).

ثالثاً: لم يحدّد القانون ما إذا كان اعتراض المكالمات أو البريد الإلكتروني يشمل **حركة البيانات** أو الاتصالات (المرسل – المرسل إليه – الوقت – المدة – الشركة المستخدمة) ام **محتوى الاتصال.** فبذكره للبريد الإلكتروني لم يحدد ما اذا كان المطلوب هو معرفة الجهات المرسلة والمتلقية فقط، أم

مصلحة وفق الأصول ذاتها وذلك خلال مهلة سبعة أيام من تاريخ تقديم المراجعة.....تضع الهيئة تقريرا سنويا يتضمن بيانًا بخلاصة أفعالها واقتراحاتها، يرفع إلى كل من رئيس الجمهورية ورئيس مجلس النواب ورئيس مجلس الوزراء.

يحدد نظام عمل الهيئة بمرسوم يُتخذ في مجلس الوزراء بناء على اقتراح رئيس مجلس الوزراء.

تنحصر مهمة التنصت بوزارة الداخلية.

أيضًا المحتوى، مع الأخذ بعين الاعتبار، أن الوصول إلى محتوى البيانات أمر في غاية التعقيد، ويحتاج إلى موافقة الشركة التي تحفظ البيانات، بالإضافة إلى مراسلة الدولة التي يتواجد فيها الServer الذي يحفظ المعلومات، أو الحصول على برامج متطورة وأصحاب خبرة تقنية عالية جداً من أجل الوصول إلى مثل هذه المعلومات الدقيقة، لذلك غالبًا ما تلجأ الأجهزة المعنية بالتحقيق إلى مصادرة الآلة(حاسوب – هاتف وغيره) توفيراً للجهد وتفاديًا للدخول في سِجالات قانونية رغم اختلاف الإجراءات القانونية بين الاثنين[60].

رغم هذه الملاحظات ما زال هذا القانون يشكل ضمانة لتأطير إجراءات اعتراض الاتصالات والمراقبة ومكافحة الجرائم الهامة المخلة بأمن الدولة والإرهاب؛ لقد ثَبُت ذلك في العديد من الإنجازات التي حققتها القوى الأمنية في الوصول إلى المجرمين والمتطرفين، ومن جهةٍ أخرى يشكل هذا القانون أساساً قانونياً للحؤول دون السماح للسلطة التنفيذية بأن تتعسف في استخدام سلطتها مع اللبنانيين عبر تفعيل النظام البوليسي فتحافظ بذلك على الخصوصية والحياة الشخصية للأفراد.

البند الثاني: بين المراقبة الإلكترونية والخصوصية الشخصية

بدأت حماية الخصوصية الفردية في القانون الدولي لحقوق الإنسان مع أواخر الستينيات من القرن المنصرم، وبالضبط في مؤتمر الأمم المتحدة لحقوق الإنسان الذي انعقد في طهران سنة ١٩٦٨، حيث خصص ورشة عمل كاملة بموضوع "تأثير التطور التكنولوجي على حقوق الإنسان".

ويطرح الإنترنت، باعتباره أهم وسيلة اتصال الآن على الصعيد العالمي، اشكالية تأثير المراقبة الإلكترونية على الخصوصية الفردية في ظل وجود تقنيات المراقبة المتطورة (كاميرات، بطاقات الهوية الإلكترونية – قواعد البيانات الشخصية ووسائل اعتراض وخرق البريد الإلكتروني وغيرها...).

وبالتالي بات من الضروري وضع الدول التشريعات اللّازمة لصون الخصوصية الفردية وضمان عدم المسّ بها، لأنها المساحة الشخصية الخاصة بكل فرد، ولأنها تحتوي على معلومات خاصة به

60 Habib, **Le droit pénal libanais à l'épreuve de la cybercriminalité** , op.cit p 193.

وسرية. وفي المقابل ليست خافية على أحد أهمية تقنيات المراقبة للحصول على الأدلة اللازمة قبل أو بعد وقوع الجريمة، أو حتى على معلومات هامة أمنية (اشتهر فيها مكتب المخابرات الخارجية في الولايات المتحدة CIA وجهاز الاستخبارات الإسرائيلية MOSSAD).

أمام هذه الإشكالية، كيف للبنان أن يحافظ على التوازن بين الضمانات لحماية الحياة الخاصة للأفراد والقدرة الأمنية العالية على الوقاية من الجرائم او اكتشاف مرتكبيها؟

بدايةً، إن الحريات مصانة في الدستور اللبناني، فهو يحمي الحرية الشخصية[61]، وحرمة المنزل الخاصة [62].

ومن خلال مشاركة لبنان في رعاية قرار الجمعية العمومية للأمم المتحدة رقم ٦٨/١٦٧ الخاص بالحق في الخصوصية، والذي اعتُمد في كانون الأول/ديسمبر ٢٠١٣، والقرار رقم ٦٩/١٦٦ الذي اعتُمد في كانون الأول/ديسمبر ٢٠١٤، يؤكدان على التزام لبنان بتعزيز احترام وضمان الحق في الخصوصية كحق من حقوق الإنسان.

كيف لا وهو من الدول الموقّعة على الإعلان العالمي لحقوق الإنسان[٦٣]، وكان أيضًا عضواً في لجنة صياغة هذا الإعلان الذي تنّص المادة ١٧ منه على أنه "لا يجوز تعريض أي شخص، على نحوٍ تعسفي أو غير قانوني، لتدخّل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته.

---

[61] **المادة ٨ في الدستور**: "الحرية الشخصية مصونة وفي حمى القانون ولا يمكن أن يقبض على أحد أو يحبس أو يوقف إلا وفاقاً لأحكام القانون ولا يمكن تحديد جرم أو تعيين عقوبة إلا بمقتضى القانون."

[62]**المادة ١٤ في الدستور**: " للمنزل حرمة ولا يسوغ لأحد بالدخول إليه إلا في الأحوال والطرق المبينة في القانون."

[٦٣] وثيقة تاريخية هامة في تاريخ حقوق الإنسان— صاغه ممثلون من مختلف الخلفيات القانونية والثقافية من جميع أنحاء العالم، واعتمدت الجمعية العامة الإعلان العالمي لحقوق الإنسان في باريس في ١٠ كانوان الأول/ ديسمبر ١٩٤٨ بموجب القرار ٢١٧ ألف بوصفه أنه المعيار المشترك الذي ينبغي أن تستهدفه كافة الشعوب والأمم. وهو يحدد،و للمرة الأولى، حقوق الإنسان الأساسية التي يتعين حمايتها عالميا. وترجمت تلك الحقوق إلى ٥٠٠ لغة من لغات العالم

ولقد جاء في قانون العقوبات: "من دخل منزلاً خلافاً الإرادة صاحبه" عوقب بالحبس [64]وكذلك من أفشى سراً علم به بحكم وظيفته أو مهنته[65].

وبالتالي لم يتم ذكر **الخصوصية الفردية الرقمية** بحد ذاتها ولكن بالقياس يتضح لنا اتجاه المشرع اللبناني إلى حمايتها من خلال المواد التي سبق ذكرها.

أضف إلى ذلك المادة الأولى من القانون١٤٠ التي تنص على أن السرية في التخابر والتواصل الجاري داخلياً وخارجياً هي حق لكل فرد ولا تخضع لأي نوع من المراقبة والتنصت أو الاعتراض إلا في حالات محددة سبق وفصلناها فيما سبق. وفي حين يبدو أن القانون يوفّر الضمانات اللّازمة لضمان الخصوصية الفردية، الّا أنَّ الممارسة تشكّل حالات الفشل المنهجي في الالتزام بالقانون وتهديداً للحق في الخصوصية للمواطنين في لبنان:

أولاً: يبدو أن الدور الفعلي للسلطة القضائية في منح التفويض أو الإشراف على التفويض الإداري للاعتراضات هو رمزي فقط لاننا حتى الآن ليس لدينا ما يدلّ على عكس ذلك وهذا الوضع مقلقٌ للغاية، إذ إن السماح لعضو في السلطة التنفيذية بإصدار تفويضٍ لاعتراض الاتصالات لا يضع ضوابط كافية، ويعتبر تطفّلًا عدوانيًا للغاية على التمتّع بالحق في الخصوصية ويقوّض المساءلة، ويزيد من احتمال حصول مراقبة تعسّفية وذات دوافع سياسية.

---

[64] **المادة ٥٧١ عقوبات لبناني:** من دخل منزل أو مسكن آخر أو ملحقات مسكنه أو منزله، خلافاً لإرادته، وكذلك من مكث في الأماكن المذكورة خلافاً لإرادة من له الحق في إقصائه، عوقب بالحبس مدة لا تتجاوز الستة أشهر.

[65] **المادة ٥٧٩ عقوبات لبناني:** من دخل منزل أو مسكن آخر أو ملحقات مسكنه أو منزله، خلافاً لإرادته، وكذلك من مكث في الأماكن المذكورة خلافاً لإرادة من له الحق في إقصائه، عوقب بالحبس مدة لا تتجاوز الستة أشهر.

من كان بحكم وضعه أو وظيفته أو مهنته أو فنه، على علم بسر وأفشاه دون سبب شرعي أو استعمله لمنفعته الخاصة أو لمنفعة آخر عوقب بالحبس سنة على الأكثر وبغرامة لا تتجاوز الأربعمائة ألف ليرة إذا كان الفعل من شأنه أن يسبب ضرراً ولو معنوياً.

إن اعتراض الجزء الأكبر من البيانات والوصول إليها هو بمثابة تحدٍّ مباشر لمبدأي الضرورة والتناسب اللذين يجب تطبيقهما لدى القيام بأي أنشطة تتعارض مع حقوق الإنسان الأساسية. وينبغي النظر إلى مراقبة الاتصالات (بما في ذلك الاعتراض والوصول إلى البيانات) كفعل يتعارض مع حقوق الإنسان ويهدّد أسس المجتمع الديمقراطي.

إن القرارات بشأن هذه الأنشطة يجب أن تأخذ بعين الاعتبار حساسية المعلومات التي يتمّ الوصول إليها وخطورة انتهاك حقوق الإنسان وسواها من المصالح المتضاربة.

ثانياً : في آذار ٢٠١٤ وافقت الحكومة على مقترح يسمح لقوى الأمن بالوصول غير المقيّد والكامل إلى بيانات الاتصالات الإلكترونية العائدة لجميع اللبنانيين. أي الحصول على كمّية كبيرة من بيانات الاتصالات العائدة إلى أربعة ملايين لبناني. وهذا يشكّل انتهاكاً للقانون، نظرًا إلى أنه لا يمكن أن يكون كل مواطن مشتبهاً به في جريمة. كما أن القرار أتاح الوصول إلى كامل المعلومات لمدة ستة أشهر، وهي أطول بكثير من مدّة الشهرين التي يسمح بها القانون ٩٠/١٤٠ بموجب المادة[66]٩.

وقد يكون مردّ ذلك عائد إلى عملية اغتيال رئيس الحكومة اللبنانية آنذاك، واختلال الأمن القومي، ودخول لبنان في سلسلة من الاغتيالات التي طالت العديد من السياسيين، وشكلت نقلة نوعية في الحياة السياسية في لبنان .

و هنا لا بد من الإشارة إلى أن الحفاظ على الخصوصية وحمايتها قانونياً ليسا فقط حكراً على أجهزة الدولة، بل يجب لتحقيقهما تنسيق التعاون بين القطاع الخاص ومزودي خدمات الإنترنت والاتصال وأجهزة الدولة الأمنية والقضائية. فالبيانات الشخصية عرضة للكشف من قبل الثلاثة وفي أي لحظة خاصةً مع التطور الحاصل الآن في المعاملات التجارية والاتصالات والنقل الرقمي للمعلومات.

---

[66] دفاع الأصوات العالمية، القانون ١٤٠: التنصّت على لبنان، ١٠ نيسان/أبريل ٢٠١٤ . متاح على:

(last revision 23/11/2019)https://ar.globalvoices.org/٢٠١٤/٠٤/١١/٣٣٤٢٤/

تجمع المؤسسات الكبرى والشركات الحكومية الكثير من البيانات والمعلومات عن الأفراد، تتعلق بالوضع المادي أو الصحي أو التعليمي أو الاجتماعي أو العمل، وتستخدم شبكات الاتصال في تخزينها ومعالجتها وتحليلها ونقلها. وهذا ما يفتح المجال إلى الإساءة في استخدامها أو مراقبة المعلومات الشخصية للأفراد وتعرية خصوصيتهم.

ولقد تأخر لبنان كثيرًا في صياغة القوانين التي تضمن حماية البيانات الرقمية الشخصية، ولكنه توصّل أخيراً بالقانون٨١ تاريخ١٠-١٠-٢٠١٨ إلى إقرار العديد من المواد القانونية الهامة، التي تحدد واجبات مزودي الخدمات التقنية وتؤكد ضرورة الحفاظ على خصوصية الأفراد أثناء معالجة بياناتهم الخاصة:

واجبات مزودي الخدمات في القانون رقم ٨١:

- على مستضيف البيانات أو مزودي الخدمات، أن يجعلوا الوصول إلى المعلومات الشخصية الرقمية مستحيلاً، إلا عند **طلب مرسل البيانات،** أو سندًا لقرارٍ من السلطة القضائية، كما ويجب عليهم الاحتفاظ بحركة بيانات المستخدمين لمدة سنتين، شرط أن تخضع للسرية المهنية، وعدم افشائها، تحت طائلة المسؤولية. على انه لا يمكن التذرع بذلك في وجه السلطة القضائية[67].
- لا يمكن لمزود الخدمات أن يزود الضابطة العدلية بالبيانات المطلوبة إلا بعد قرار من السلطة القضائية المختصة. ولكن للضابطة العدلية أن تطلب منه حفظ البيانات لمدة أقصاها ثلاثون

[67] **المادة ٦٩ من القانون ٨١ تاريخ ١٠-١٠-٢٠١٨** :لا يلزم مقدّم خدمة الاتصال بمراقبة المعلومات التي يرسلها أو التي يخزنها مؤقتاً. إنما يتوجب عليه فورا تحت طائلة المسؤولية، أن يسحب المعلومات المخزّنة مؤقتاً أو أن يجعل الوصول إليها مستحيلاً بناء على طلب مرسل المعلومات أو بناءً على قرار من السلطة القضائية.

المادة ٧٠ من القانون نفسه:لا يلزم مستضيف البيانات بمراقبة المعلومات التي يخزنها من أجل وضعها في تصرف الجمهور، إنما تترتب عليه المسؤولية إذا لم يسحب هذه المعلومات أو إذا لم يجعل الولوج إليها مستحيلاً فور معرفته الفعلية بطابعها غير المشروع الظاهر جلياً.

يوماً إضافيًا لما هو منصوص عنه. وذلك لضمان عدم فقدان أو تعديل البيانات الرقمية وخاصةً إذا وجد طابع العجلة.[68]

- والجدير ذكره، أن موجب الحفظ المنصوص عليه، لا يشمل المحتوى أو المضمون المخزن أو المنقول، بل فقط حركة البيانات، ولقد تحدثنا عن الفرق بين الإثنين سابقاً.
- لقد جاء هذا القانون ليجمع بين القانون٩٠/١٤٠ ودور مستضيفي البيانات، بحيث نص في في المادة ٧٦ على وجوب التعاون مع القضاء المختص، ضمن حدود إظهار الحقيقة، وتنفيذاً لموجب الحفظ المنصوص عنه، وحتى الوصول إلى المعلومات المذكورة وفقاً للوقت الحقيقي لأي عملية اتصال عبر شبكته.[69]

---

[68] **المادة ٧٢ من القانون ٨١ تاريخ ١٠-١٠-٢٠١٨**..... للضابطة العدلية في إطار إجراءات تحقيق في دعوى جزائية،وبعد اعلام المرجع القضائي المختص، الطلب من مقدمي الخدمات التقنية حفظ بيانات تقنية إضافية لما هو منصوص عليه في الفقرة الأولى من هذه المادة لمدة أقصاها ثلاثون يوماً وبشأن واقعة محددة وأشخاص محددين، وذلك بالنظر إلى طابع العجلة وإمكانية تعرّض هذه البيانات للفقدان او التعديل. لا تسلّم هذه البيانات إلى الضابطة العدلية الا بقرار من المرجع القضائي المختص.....

[69]_**المادة ٧٦ من القانون٨١ تاريخ ٢٠١٨/١٠/١٠:** على مقدمي الخدمات التقنية التعاون مع القضاء المختص والمراجع المنصوص عنها في القانون رقم ٩٩/١٤٠ وضمن حدود لإظهار الحقيقة في كل تحقيق يجريه أو في كل دعوى عالقة أمامه.

للقضاء المختص والمراجع المنصوص عليها في القانون رقم ١٤٠/٩٩ وضمن حدوده، في اطار تحقيق أو دعوى، ان تُلزم مقدم الخدمات التقنية بتسليمها البيانات التي في حوزته أو الموضوعة تحت رقابته، تنفيذاً لموجبي الحفظ المنصوص عليهما في المادتين ٧٢ و٧٤ من هذا القانون، وذلك في حدود مقتضيات التحقيقات والمحاكمات.

الحفاظ على الخصوصية أثناء معالجة البيانات الخاصة:

تناول هذا القانون في الفصل الخامس منه، موضوع معالجة البيانات الخاصة ذات الطابع الشخصي، مشدداً على ضرورة الحفاظ عليها والتعاطي معها بأمانة، ولغايات مشروعة ومحددة وعدم الكشف عنها لأشخاص غير المخولين بالاطلاع عليها منعًا لإساءة استخدامها أو تشويهها.[70]

وللأشخاص الذين أعطوا هذه المعلومات أن يعلموا التفاصيل كافة عن الجهة التي تجمع المعلومات وتعالجها. وله الاعتراض على ذلك [71] كما وتم وضع شروط أساسية وضوابط يجب الالتزام بها عند الجمع فمثلاً يمنع القيام بذلك إذا كانت البيانات تتناول الحالة الصحية أو الهوية الوراثية أو الحياة الجنسية، لما في ذلك من خصوصية كبيرة قد يؤدي الكشف عنها إلى أضرار وخلل اجتماعي خاصةً في مجتمعاتنا.

وهناك حالات معينة لا يسري عليها هذا المنع، ومنها الحصول على ترخيص مسبق، وهو عبارة عن قرار تصدره الوزارة المعنية. فوزارة الدفاع الوطني ووزارة الداخلية تعنيان بإصدار القرار بالترخيص بجمع ومعالجة البيانات المتعلقة بالأمن الداخلي والخارجي، ووزارة العدل للبيانات المتعلقة بالجرائم

---

[70] **المادة ٨٧ من القانون نفسه:** تُجمع البيانات ذات الطابع الشخصي بأمانة ولأهداف مشروعة ومحددة وصريحة.

يجب أن تكون البيانات ملائمة وغير متجاوزة للأهداف المعلنة، وأن تكون صحيحة وكاملة وأن تبقى ميوّمة بالقدر اللازم. لا يمكن في مرحلة لاحقة معالجة هذه البيانات لأهداف لا تتوافق مع الغايات المعلنة، ما لم يتعلق الأمر بمعالجة بيانات لأهداف إحصائية أو تاريخية أو للبحث العلمي.

[71] **المادة ٩٢ من القانون ٨١ تاريخ ١٠-١٠-٢٠١٨** : لكل شخص طبيعي الحق في الاعتراض لأسباب مشروعة، أمام المسؤول عن المعالجة على تجميع البيانات ذات الطابع الشخصي الخاصة به ومعالجتها، بما في ذلك التجميع والمعالجة بهدف الترويج التجاري. إلا أنه لا يحق للشخص ممارسة حق الاعتراض في الحالتين التاليتين:

١- إذا كان المسؤول عن معالجة البيانات ملزماً بجمعها بمقتضى القانون.

٢- إذا كان قد وافق على معالجة البيانات ذات الطابع الشخصي الخاصة به.

الجزائية والدعاوى القضائية ووزارة الصحة بالحالات الصحية. على أن يتم تبليغ نتيجة القرار إلى مقدم الطلب وإلى وزارة الاقتصاد والتجارة (ولم نفهم الغاية من ذلك).

ولقد أعفى القانون التقدم بأي طلب تصريح في حالات عديدة نصت عليها المادة ٩٤ من القانون رقم ٨١ وابرزها المعالجات التي يجريها أشخاص الحق العام والمعالجات المنصوص عنها في القانون ١٤٠/٩٩.[72]

من هنا نرى الاتجاه الواضح للمشرع اللبناني الى فرض ما أمكن من المواد القانونية، للحفاظ على خصوصية البيانات الشخصية للمواطنين، تماشياً مع الاتجاه الدولي والإقليمي (الأوروبي) ، نحو حياة أكثر خصوصية، كما فعلت العديد من الدول. ففي الولايات المتحدة الأميركية نظم قانون خصوصية الاتصالات الإلكترونية سنة ١٩٨٦ **Electronic Communications Privacy Act of 1986 (ECPA)**[٧٣] كيفية حصول أجهزة الدولة على المعلومات المخزنة عند مزودي الخدمات، فاعطى الحق لرجل الضبط القضائي في الحصول على المعلومات الاساسية

---

[72] المادة ٩٤ من القانون نفسه :لا يتوجب التقدم بأي تصريح أو طلب أي ترخيص لمعالجة بيانات ذات طابع شخصي في الحالات التالية:

١– في المعالجات التي يجريها أشخاص الحق العام كل في نطاق صلاحياته.

٢– في حال قيام جمعيات لا تبغي الربح، بمسك السجلات الخاصة بأعضائها والمتعاملين معها ضمن نطاق ممارستها بشكل طبيعي وقانوني لمهامها.

٣– في المعالجات التي يكون موضوعها مسك سجلات مخصصة، بموجب أحكام قانونية أو تنظيمية، لإعلام الجمهور والتي يمكن ان يطلع عليها كل شخص او أشخاص لهم مصلحة مشروعة.

٤– في المعالجات التي يكون موضوعها التلاميذ والطلاب من قبل المؤسسات التربوية لغايات تربوية أو إدارية خاصة بالمؤسسة. ......

[73] https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285(Last revision 12/1/2020)

للمشترك (الاسم والعنوان)، أو المعلومات المتعلقة ببريده الإلكتروني أو بريده الصوتي، بمجرد توجيه أمر من المحكمة إلى مزود خدمة الإنترنت تأمره بالكشف عن محتويات الحاسب[٧٤].

و سنة ٢٠٠٤ في فرنسا أصدر المشرع الفرنسي:

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique[75]

حيث فرض على مزودي الخدمات المساعدة في مكافحة الجرائم ضد الإنسانية والاستغلال الجنسي للأطفال وغيرها من الجرائم الهامة من خلال مراقبة حركة مستخدمي الإنترنت.[76]

---

[74]**Electronic Communications Privacy Act of 1986 (ECPA) TITLE II**–STORED WIRE AND ELECTRONIC COMMUNICA TIONS AND TRANSACTIONAL RECORDS ACCESS"**CHAPTER 121** STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS n°2703: Requirements for governmental access.

[75] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164 (derniere visite 14/12/2019)

[76]**Article 6** Modifié par LoI n°2018-898 du 23 octobre 2018 - art. 29 "..7.Les personnes mentionnées aux 1 et 2 ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites.

Le précédent alinéa est sans préjudice de toute activité de surveillance ciblée et temporaire demandée par l'autorité judiciaire.

Compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de la provocation à la commission d'actes de terrorisme et de leur apologie, de l'incitation à la haine raciale, à la haine à l'égard de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap ainsi que de la

في الخلاصة لا بُدّ من العمل دائمًا على إيجاد التوازن بين حفظ الأمن والاستقرار الأمني في الوطن ومكافحة الجرائم المخلة به والإرهاب، وبين عدم شعور المواطنين بأن بياناتهم الشخصية وخصوصيتهم عرضة للخرق في أي لحظة من قبل أجهزة الدولة أو شركات القطاع الخاص وهذا التوازن لا يتحقق إلا من خلال السيطرة المستمرة على إجراءات الضابطة العدلية والأجهزة الأمنية لضمان حماية الخصوصية الفردية.

في نهاية هذا القسم، وبعد عرض ما سبق يتبين لنا أنه تم القيام بالعديد من الخطوات والإجراءات الهامة في لبنان من أجل مواكبة التطور التقني مع دخول العالم الرقمي إلى عالم الإجرام.

فعلى الصعيد الأمني تم تطوير قوى الأمن الداخلي من خلال استحداث مكاتب متخصصة في الشرطة القضائية، تعنى برفع الأدلة الرقمية وتحليلها، مثل مكتب الأعتدة واللوازم في المباحث

---

pornographie enfantine, de l'incitation à la violence, notamment l'incitation aux violences sexuelles et sexistes, ainsi que des atteintes à la dignité humaine, les personnes mentionnées ci-dessus doivent concourir à la lutte contre la diffusion des infractions visées aux cinquième, septième et huitième alinéas de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et aux articles 222-33, 225-4-1, 225-5, 225-6, 227-23 et 227-24 et 421-2-5 du code pénal.

A ce titre, elles doivent mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données. Elles ont également l'obligation, d'une part, d'informer promptement les autorités publiques compétentes de toutes activités illicites mentionnées à l'alinéa précédent qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part, de rendre publics les moyens qu'elles consacrent à la lutte contre ces activités illicites.

الجنائية العلمية، ومكتب مكافحة جرائم المعلوماتية. بالاضافة إلى توسيع صلاحيات شعبة المعلومات في هذا المجال، من خلال استحداث الفرع الفني فيها الذي كان السبب في العديد من الإنجازات الأمنية.

اما بالنسبة إلى دور القطاع الخاص، فلقد نظّم القانون رقم ٨١ الذي صدر مؤخراً في ٢٠١٨/١٠/١٠ واجبات مزودي الخدمات التقنية، وأهمها حفظ حركة بيانات المستخدمين والمشتركين، وتزويد القضاء بما يلزم، بغية مكافحة الجريمة الإلكترونية ومعرفة الموقع الجغرافي للفاعلين. وفي المقابل تأمين الحماية اللازمة للبيانات الرقمية من أجل ضمان خصوصية الحياة الخاصة، وعدم إفشائها إلا في حالات محددة في القانون نفسه.

وبالنسبة إلى إجراءات التفتيش والمصادرة، فلقد شرحنا الصعوبات التي تواجه الضابطة العدلية والقضاء أثناء رفع الأدلة الرقمية المخزّنة في أنظمة المعلومات من الناحيتين التقنية والقانونية. وبالأخصّ عند الولوج إلى انظمة أخرى متباعدة جغرافياً أو أثناء اعتراض حزمات البيانات الرقمية المتطايرة في الوقت الحقيقي للإرسال. ولقد جاء القانون رقم ٨١ المذكور ليضع حدًا للعديد من الاشكاليات التي كانت مطروحة. إلا أنه مازال في حاجة إلى تحسين اكثر وتعديل في ما يتعلق بمشروعية المراقبة الإلكترونية وكيفية تنفيذها. لأن القانون رقم ٩٩/١٤٠ تناول التنصت على المكالمات الهاتفية بشكل أساسي ولم يعالج موضوع المراقبة الإلكترونية وحركة البيانات الرقمية.

تشكل هذه الصعوبات تحدياتٍ كبيرةً للقضاء والتشريع اللبناني على الصعيد الداخلي، إذ إن أي خلل في إجراءات رفع الأدلة الرقمية وحفظها قد تعرضها للتلف والتشويه أو لفقدان مصداقيتها ونزاهتها. وبالتالي تقلّ قيمتها الثبوتية أمام القاضي أو حتى لا يؤخذ بها إطلاقاً.

ونظرًا لطبيعة العالم السيبراني اللامحدود وإمكانية انتقال البيانات الرقمية بسرعة كبيرة بين الدول، تظهر عقبة مهمة أثناء التحقيقات الا وهي وجود الأدلة الرقمية في نظام معلوماتي رقمي خارج الأراضي الإقليمية حيث لا بُدّ من اعتماد سبل التعاون الدولي الشرطي والقضائي كافة لضمان عدم فرار مرتكبي جرائم المعلوماتية من العقاب مستغلين الحدود الجغرافية الدولية.

لذلك سيتركز القسم الثاني من بحثنا حول موضوعين أساسيين: الأول هو القوة الثبوتية التي يتمتع بها الدليل الرقمي أمام المحكمة والثاني يتحدد بدور التعاون الدولي الشرطي من ناحية، والقضائي من ناحية أخرى في جمع الدليل الرقمي وأهمية الإتفاقية الدولية للجريمة الإلكترونية التي أبرمت في بودابست سنة ٢٠٠١ في تفعيل المساعدة القانونية المتبادلة.

القسم الثاني: التحديات التي تفرضها حداثة الدليل الرقمي على القضاء

يواجه لبنان تحديات كبيرة في مجال التعامل مع الدليل الرقمي، نظرًا إلى خصوصية هذا النوع من الأدلة وطبيعتها المختلفة عن الأدلة التي اعتادت الأجهزة الأمنية والقضاء على التعامل بها. ولعل هذه التحديات سوف تزول في الأيام المقبلة لأن اطلاع الأجيال الناشئة على العالم الرقمي أصبح من الحياة اليومية، ولن تواجه الصعوبات التي يواجهها اليوم الجيل الحالي من القضاة والضباط من أصحاب الرتب العالية في الأجهزة الأمنية.

تتجسد هذه التحديات على صعيدين، وطني ودولي:

فعلى الصعيد الوطني يبرز التحدي الأكبر، ليس في جمع الدليل الرقمي فحسب بل في اتباع الأسس الصحيحة التي تضمن نزاهته وعدم تعرضه للتشويه والتحريف أثناء عملية رفع الأدلة، ومن ثم إبقائه في ظروف صحية تضمن وصوله إلى المحكمة بالصورة المطلوبة.

بالإضافة إلى ذلك، فإن تعامل القاضي الجزائي اللبناني مع الأدلة الرقمية يشوبه الكثير من العيوب النابعة من عدم إلمام أغلب القضاة العالم الإلكتروني الرقمي وغياب الوقت الكافي لإجراء دورات تدريبية مستمرة، تعزز من قدرة القاضي على الاقتناع بالدليل الرقمي وتفعّل سلطته التقديرية في قبول الدليل أو عدمه. وسيكون ذلك موضوع الفصل الأول من هذا القسم.

وعلى الصعيد الدولي، تظهر الحاجة الملحة إلى التعاون الدولي في عملية جمع الأدلة الرقمية، التي غالبا ما تكون موجودة ومخزنة في انظمة رقمية خارج الأرض الإقليمية للدولة اللبنانية، مع الأخذ بعين الاعتبار ان لبنان ليس من الدول الموقعة على إتفاقية بودابست المعنيّة بالمساعدة القانونية المتبادلة بين الدول واسترداد المجرمين. وسنشرح ذلك في الفصل الثاني من هذا القسم.

الفصل الأول القوة الثبوتية للدليل الرقمي أمام القضاء

بعد ان عرضنا بإسهاب آلية جمع الدليل الرقمي، والإطار القانوني لذلك، أكان داخل مكونات الآلة أم نظام المعلومات حيث يتم الحصول على الدليل، من خلال إجراءات التفتيش والمصادرة والدخول إلى أنظمة أخرى عن بعد، أو الحصول عليه من خلال اعتراض حزمات المعلومات والاتصالات أو (ما يعرف بالمراقبة الإلكترونية).

لا بُدّ من القول بأن عملية جمع الأدلة الرقمية صعبة وفي غاية الدقة، وهي تحتاج إلى تعاون كبير بين أجهزة الدولة الرسمية والقطاع الخاص والخبراء. الّا أنَّ كل ذلك، ومع أهميته في مرحلة التحقيق، لا يشكل إلا المرحلة الأولى من العملية إذ إنه لا يكفي أن نحصل على الدليل الرقمي فحسب بل يجب معرفة كيفية الحفاظ عليه وعلى سلامته وموثوقيته، ومعرفة الإطار القانوني في حفظه لحين عرضه أمام القاضي تحت طائلة عدم قبوله.

هذا من ناحية، أما من ناحية أخرى فإن تأثير الدليل الرقمي على القاضي، له الدور الكبير في إحقاق الحق، إذ إنه قد يغير المعطيات كلها مقابل عدم إلمام بعض القضاة بتعقيدات العالم الرقمي.

لذلك تنقسم الدراسة في هذا الفصل إلى مبحثين، يكون موضوع الأول قبول القاضي الدليل الرقمي من الناحية القانونية والمضمون، ويكون موضوع الثاني تأثير الدليل الرقمي على سلطة القاضي التقديرية.

<u>المبحث الأول</u>: قبول الدليل من قبل القاضي

كثيرة هي طرق الإثبات في الدعاوى الجزائية، ولكل منها أهميتها ودورها في تكوين قناعة القاضي بحسب المادة ١٧٩ من قانون أصول المحاكمات الجزائية [77] منها ما هو مباشر مثل الاعتراف والشهادة والخبرة والإثبات الخطي بالإضافة إلى سلطة القاضي التقديرية المرتكزة على معلوماته الشخصية، ومنها ما هو غير مباشر أو ما يسمى بالقرائن واستنتاج واقعة غير معروفة من وقائع أخرى معروفة مرتبطة بها ارتباطاً وثيقاً. قد تكون قاطعة مثل القرائن القانونية (القاصر دون السابعة من العمر الذي لا يعاقب على أي جريمة) وقد تكون متروكة لسلطة القاضي التقديرية، بحيث يستخلصها من ظروف كل قضية، ويصح الاستناد إليها في تعزيز الأدلة الأخرى القائمة في الدعوى؛ ومثال على ذلك توجيه المتهم التهديدات عبر الفايسبوك إلى المجني عليه قبل الحادث، شراء السلاح عبر موقع "Amazon" قبل وقت قريب من الجرم، دخول المتهم إلى مواقع رقمية متعلقة تدل على اضطراب نفسي أو هوس معين الخ.....

و بالتالي يمكن القول إن أغلب الأدلة الرقمية تنطوي تحت خانة القرائن التقديرية في الدعاوى الجزائية، وتهدف بشكلٍ أساسي إلى تكوين قناعة عند القاضي لإصدار الحكم.

وهنا لا بُدّ من التمييز بين نوعين من الأنظمة القانونية: النظام اللاتيني[78] والنظام الانكلوساكسوني[79].

---

[77] **المادة ١٧٩ أ.م.ج:** يمكن اثبات الجرائم المدعى بها بطرق الإثبات كافة ما لم يرد نص مخالف. لا يمكن للقاضي أن يبني حكمه إلا على الأدلة التي توافرت لديه شرط أن تكون قد وضعت قيد المناقشة العلنية أثناء المحاكمة. يقدر القاضي الأدلة بهدف ترسيخ قناعته الشخصية.

[78] النمسا والدنمارك، فنلندا، ألمانيا، فرنسا، اليابان، البرتغال، النرويج، والسويد...

[79] استراليا وكندا والولايات المتحدة الأميركية وبريطانيا ...

إن مصدر قواعد الإثبات في النظام الإنكلوساكسوني هو القانون العادي الإنكليزي القديم، المبني على العرف والعادة Common law، والذي يوجب التقيد بقاعدتين قديمتين قد تعيقان الإثبات بواسطة المستندات المعلوماتية وتجردها من القيمة الثبوتية المطلوبة:

أولاً: قاعدة الإثبات الأفضل Best Evidence Rule أو قاعدة الأصل (La Meilleure preuve) التي تلزم القاضي بأن يأخذ في عين الاعتبار الإثبات الأفضل الذي يمكن لطرف ما أن يقدمه إليه ويفهم به الأصل، أو النسخة الأصلية للمستند، وغالبًا ما يكون ذلك غير متوفر في المستندات الرقمية. فمثلًا يتعذر إثبات وجود عقد حاصل ألكترونياً بواسطة البريد الإلكتروني، من خلال طباعة نسخة الرسالة الإلكترونية المتضمنة لهذا العقد، لأن الأخير ليس سوى نسخة عادية عن الأصل المتكون من البيانات الإلكترونية الرقمية. كما يتعذر إثباتها من خلال تقديم البيانات في شكلها الرقمي لكونها غير قابلة للقراءة إلا بعد الاستعانة بالحاسب الآلي.[80]

لذلك وحصرًا للنقاش في الولايات المتحدة جاء قانون الإثبات الفيدرالي Federal Rules Of Evidences[81] ليوحّد قواعد الإثبات في الولايات المتحدة الأميركية والذي استكمل لاحقاً بصدور قانون فدرالي متخصص بالتوقيع الإلكتروني ضمن نطاق التجارة الداخلية والعالمية صدر في ٣٠ حزيران عام ٢٠٠٠، ونص صراحة على أن التسجيلات الرقمية، وكل شكل آخر يستخدم في جمع البيانات، يعتبر بمثابة الصيغة الخطية الأصلية لكل طباعة ورقية للتسجيلات الرقمية شرط أن تنقل بشكل آمن وسليم.

ثانيًا: قاعدة عدم جواز الإثبات بما يسمع أو يقال أو يشاع Hearsay Rule أو Ouï-dire بالفرنسية:

---

[80] عيسى، **التنظيم القانوني لشبكة الإنترنت**، مرجع سابق ص٣٥٢.

[81] https://www.uscourts.gov/sites/default/files/evidence-rules-procedure-dec2017_0.pdf(last revision 20/12/2019)

تمنع قاعدة عدم جواز الإثبات بما يقال أو يشاع لأن الإثبات أتى بواسطة مستند غير أصلي، ما لم يكن صاحب هذا المستند على عِلم شخصي بمضمون هذا المستند، بعد أن يشهد هذا الأخير بذلك في المحكمة. وهذه القاعدة تشكل عائقًا أمام القاضي لقبول الدليل الرقمي. لذلك فرض قانون الإثبات الفدرالي استثناءً على هذه القاعدة، تماشياً مع نظام المعلومات المتطور والإنترنت، واعتبر أن المستند الرقمي الذي سبق وتشكل في نطاق النشاط العادي لشركة معينة يمكن أن يقبل به كوسيلة للإثبات، إنما بشرط أخذ شهادة شخص على اطلاع على نظام تسجيل وحفظ البيانات وعلى كل ما يتصل بموثوقية النظام المعلوماتي القائم[82].

ونرى هنا بشكل واضح، الاتجاه العام في النظام الانكلوساكسوني إلى تسهيل عملية الإثبات الإلكتروني والرقمي، تماشيًا مع النظام الرقمي والإنترنت، خاصةً وأن طريقة التواصل عبر الإنترنت، بدأت أولًا في الدول التي تتبع هذا النظام القانوني(الولايات المتحدة الأميركية وبريطانيا)

في المقابل، النظام اللاتيني قائم على حرية الإثبات في القضايا الجزائية، وهذا ما يسهل أكثر قبول الدليل من قبل المحكمة، واقتناع القاضي، شرط الحصول على الإثبات بطريقة صحيحة وشرعية[٨٣].

أما السؤال المطروح: هل كل معلومة أو دليل رقمي صادر عن نظام معلوماتي معين مقبول للنظر به أمام المحكمة في الأنظمة اللاتينية؟ كيف يضمن القاضي أن هذا الدليل موثوق وسليم؟ ما هو تأثير إجراءات الضابط العدلية على مشروعية الدليل الرقمي؟

سنبحث في هذه الاسئلة بالتفصيل خاصةً وأن لبنان ما زال حديث العهد في هذا المجال ويرتكز على القوانين الفرنسية كنموذج لتطوير التشريع ومواكبة العالم الرقمي والإنترنت.

---

[82] Federal Rules of Evidence , Rule 801 802 : Dahl's Law dictionary Compiled by Henry Saint Dhal , Hein et Dalloz 1995.

[٨٣] الخوري (جنان)، الجرائم الاقتصادية الدولية والجرائم المنظمة العابرة للحدود، الطبعة الأولى، مكتبة صادر ناشرون، سنة ٢٠٠٩ ص ٣١٩.

البند الأول: مشروعية الدليل الرقمي في لبنان

جاء في المادة ١٧٩ من أصول المحاكمات الجزائية في لبنان :" يمكن إثبات الجرائم المدعى بها بكافة طرق الإثبات ما لم يرد نص مخالف " ما يدل على أن جميع الأدلة التي تعرض في المسائل الجزائية مشروعة. قد يُعمل بهذه المادة في الجرائم التقليدية، حيث للقاضي السلطة المطلقة بقبول الدليل أو رفضه.

ولكن مع دخول العالم الرقمي والإنترنت إلى الحياة اليومية، لم تعد النصوص القانونية التقليدية في الإثبات متناسبة مع متطلبات التطور التكنولوجي المتسارع، لا لجهة إمكانية قبول المستندات الإلكترونية غير المادية كوسيلة للاثبات، ولا لجهة منح هذه المستندات قوة ثبوتية أو حجية ملزمة.

من هنا برزت الحاجة إلى تطوير النصوص المتعلقة بالإثبات الإلكتروني فتم إقرار القانون رقم٨١ تاريخ ٢٠١٨/١٠/١٠:

١- لقد هدف هذا القانون إلى إضفاء تعريف جديد للإثبات الخطي، لكي يشمل السند الإلكتروني، وأزال الالتباس القانوني الناشئ عن الخلط بين الكتابة (الخطي) وبين ما هو ورقي أي الركيزة التي يتجسد الخطي بواسطتها، فجاءت المادة الرابعة فيه، لتقرّ بالمفاعيل القانونية التي تنتج عن التوقيع الإلكتروني، شرط أن يكون ممكن تحديدُ الشخص الذي صدر عنه، وأن تُحفظ بطريقة تضمن سلامتها وهي المادة نفسها رقم ١٣١٦-١ في القانون الفرنسي.[84]

---

[84] **Article 1316-1** (inséré par Loi 2000-230 du 13 mars 2000 art. 1 Journal Officiel du 14 mars 2000) L'écrit sous forme électronique est admission en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il so établi et conservé dans des conditions de nature à en garantir l'intégrité.

٢- للسند الرقمي القوة الثبوتية ذاتها التي للسند الخطي المدوّن على الورق.[85]

يأتي تركيز هذا القانون على السندات والعقود الرقمية بشكل أساسي ولعل الدافع هو إضفاء نوع من الأمان على المعاملات التجارية وتبادل الصفقات التجارية بين الشركات، التي تستخدم العالم السيبراني في معرض نشاطاتها، وما يعكس إيجابية على الاقتصاد اللبناني.

أما بالنسبة للأدلة الرقمية الأخرى، مثل التسجيلات الصوتية وحركة البيانات وغيرها، فمن الواضح أنه ترك للمحكمة السلطة التقديرية الكاملة بقبولها او رفضها، وذلك حسب ظروف الدعوى ونوع الجرم.

في إطار المشروعية، على الضابط العدلي الذي يجمع الأدلة التقيد بمضمون المواد المتعلقة بالتفتيش والمصادرة في أصول المحاكمات الجزائية التي سبق وفصلناها بإسهاب، والتقيد بمضمون القانون ٨١ المذكور تحت طائلة ملاحقة الضابط العدلي، وإبطال المعاملة المذكورة من دون بقية الإجراءات.

والسؤال هنا: ماذا لو وجد الضابط العدلي أثناء تفتيشه "المخالف" لنظام المعلومات للمشتبه به وبشكل غير قانوني، ادلة رقمية تفيد التحقيق؟ هل يتم قبولها في المحكمة؟ أم تفقد مشروعيتها؟

في هذه الحالة، يعود للقاضي أن يأخذ بها على سبيل المعلومات على أن يتم تدعيمها بأدلة أخرى ولا يكتفى بها لوحدها[86].

---

[85] **المادة ٧ من القانون ٨١ تاريخ ١٠-١٠-٢٠١٨** : يقبل السند الإلكتروني في الإثبات وتكون له المرتبة والقوة الثبوتية ذاتها اللتان يتمتع بهما السند الخطي المدون على الورق، شرط ان يكون ممكناً تحديد الشخص الصادر عنه هذا السند وان ينظم ويحفظ بطريقة تضمن سلامته.

[86] نصر (فيلومين)،أصول المحاكمات الجزائية، دراسة مقارنة وتحليل، الطبعة الأولى ٢٠١٣، المؤسسة الحديثة للكتاب ص ٥٢٣.

البند الثاني: سلامة الدليل أثناء نسخه وتخزينه

إن إزالة العوائق القانونية التي تعترض إمكانية قبول الإثبات الرقمي بالمستندات الإلكترونية، يستدعي من جميع الدول إدخال التعديلات التشريعية على الأنظمة القانونية المختلفة المعمول بها في مجال الإثبات. ولكن أن يكون الدليل الرقمي مقبولًا كوسيلة للإثبات شيء، وأن يكون محتواه موثوقًا وغيرَ مشكوكٍ به أمر آخر. فكل ما كان الدليل الرقمي نزيهًا (بمصدره وسلامة حفظه وعدم التلاعب به لحين عرضه أمام المحكمة) كلما زادت قوته الثبوتية.

و حتى في ظل قاعدة حرية الإثبات في القضايا الجزائية، والأهمية الكبرى لسلطة القاضي التقديرية في البحث في الأدلة الرقمية، إلّا أنَّه لا يجب الاستخفاف بمدى تاثير موثوقية الدليل وقيمته الثبوتية في قناعة القاضي الشخصية.

و هنا يتحول الإشكال بالإثبات الرقمي هنا من إشكال قانوني إلى إشكال تقني يرتبط بالعديد من الإجراءات التقنية الهادفة لضمان سلامة الدليل وأهمها:

اعتماد نظام معلوماتي موثوق به، واستخدام أدوات تشفير أثناء حفظ الدليل(Hashing) وتعميم آلية مصادقة شخص ثالث.

- **موثوقية النظام المعلوماتي:**

تعتمد القوة الثبوتية للدليل الرقمي، إلى حد بعيد على موثوقية نظام المعلومات المستخدم. وهنا لا بد من إلقاء الضوء في هذا المجال على التجربة الكندية النموذجية في هذا المجال، بحيث اعتبرت أن المعلومات المدونة على قاعدة معلوماتية، يمكن نسخها، ويكون لها الحجية الكافية إذا كان المستند مفهوم المحتوى مع الأخذ بعين الاعتبار الظروف التي سجلت فيها البيانات فيها ونُسخت في ظلها.

كما وأن تسجيل بيانات العمل القانوني، على قاعدة معلوماتية، فيه جميع الضمانات الجدية الكافية للوثوق فيه، حين يكون التسجيل حاصلاً بطريقة منهجية وخالية من الهفوات، وحين تكون البيانات المسجلة محمية من العيوب[87].

وهنا لا بُدّ من عرض رأي الفقيهة الفرنسية **Sédaillan** [88] التي قسمت مقومات منح نظام المعلومات الموثوقية الكافية إلى أربع درجات:

- في الدرجة الأولى: يجب أن يسمح النظام الرقمي بتوفير الضمانات اللّازمة لحسن أدائه، بحيث يسمح للقضاة منح ثقة أكبر للتسجيلات المعلوماتية والمستندات المسحوبة من الحاسب الآلي.

- في الدرجة الثانية : يجب أن يضمن حفظاً منهجياً ومنظماً لجميع العمليات المعلوماتية الحاصلة، واستخدام وسائط التخزين التي لا تقبل التغيير مثل الاسطوانات الضوئية غير القابلة لإعادة التسجيل لضمان عدم تعريض الدولة لتعديلات إرادية أو غير إرادية أثناء الحفظ.

- في الدرجة الثالثة :اعتماد نظام قادر على جعل وسائط التخزين حيث البيانات مسجلة، يرصد عدد المرات التي تُجرى فيها المعاينة، ومبرر ذلك ضبط الإمكانية التقنية في نسخ البيانات الرقمية التي تبقى موجودة.

- في الدرجة الرابعة: يجب أن يَسمح النظام المعلوماتي بإجراء تحديد دقيق لتاريخ إرسال واستلام المستندات المعلوماتية والتأكد من كونها استلمت من قبل من أرسلت إليه من دون تعديل أو مس بسلامتها.

---

[87] عيسى، **التنظيم القانوني لشبكة الإنترنت**، مرجع سابق ص ٣٥٧

[88] Sédaillan (Valerie) DROIT DE L'INTERNET: Réglementation, responsabilités, contrats, collection AUI, janvier 1997, p207

,

مع العلم بانه ليس هناك من نظام معلوماتي يؤمن جميع شروط الأمان، وما من شيء ينفي احتمال مواجهة خلل أو عيوبٍ ما.

استخدام أدوات تشفير البصمة الرقمية أثناء حفظ الدليل.

يفهم التشفير أو الترميز بانه الآلية التي بمقتضاها تترجم معلومات مفهومة إلى معلومات غير مفهومة، عبر تطبيق بروتوكولات سرية قابلة للانعكاس(أي يمكن إرجاعها إلى حالتها الأصلية) وهي تقنية قوامها خوارزميات رياضية ذكية، تسمح لمن يمتلك مفتاحاً رقمياً سرياً، أن يحوّل رسالة مقروءة إلى غير مقروءة و بالعكس. أي أن يستخدم المفتاح لفك الشيفرة وإعادة الرسالة المشفرة إلى وضعيتها الأساسية.[89]

لن ندخل أكثر في تقنيات التشفير إذ إنها واسعة ومعقدة، ولكن الغاية من عرض هذا التعريف، هو إلقاء الضوء على أهمية هذه التقنية، في الحفاظ على سلامة الدليل، وضمان عدم المس بمحتواه. فإذا قامت الضابطة العدلية بعد جمع الدليل الرقمي بتشفير محتواه، ومنع قراءة هذا المحتوى أو تعديله الى حين عرضه، فهذا يزيد من موثوقيته وقبوله أمام القضاء وإلا فقد تكون الإجراءات كافة التي اتخذتها من أجل كشف الحقيقة عرضة لعدم قبولها في المحكمة.

و الآن أصبحت معظم الدول(طبعاً لبنان ليس ضمنها) تعتمد تقنية البصمة الرقمية لكل ملف رقمي يتم حفظه كدليل، وفي حال حصل أي تعديل أو دخول أو معاينة لهذا الملف تتغير البصمة الرقمية(HASH) الممنوحة من قبل الضابط العدلي أو من الذي قام برفع الدليل، وبالتالي فعند عرضه في أمام المحكمة لا بُدّ أن تكون البصمة هي نفسها، وعلى القاضي التأكد من ذلك من أجل ضمان الموثوقية.

---

[89] عيسى، التنظيم القانوني لشبكة الإنترنت، مرجع سابق ص ٢٠٠

أشهر التطبيقات في هذا المجال هي الـ MD5 و SHA1[90] ونعطي مثالًا على ذلك :

البصمة الرقمية عبر الـ MD5 عند رفع الدليل	A٦٤C٠C٦٦٨٨٧٧٢١٤٥٦
البصمة الرقمية عبر الـ MD5 عند العرض أمام المحكمة	A٦٤C٠C٦٦٨٨٧٧٢١٤٥٦

هنا نرى أن البصمة ما زالت نفسها، وهذا يعني أن الدليل لم يُمسَّ به في فترةِ حِفظه. أما لو وجد رقم أو حَرف واحد متغيّر في البصمة التي يوجد تطبيقات خاصةً لمقارنتها، فهذا كفيل بعدم قبوله أمام المحكمة.

آلية مصادقة شخص ثالث

يمكن تعريف الشخص الثالث المصادق على أنه هيئة أو جهة عامة أو خاصة تصدر الشهادات الإلكترونية، وهي كناية عن سجل معلوماتي يحتوي على مجموعة من المعلومات التعريفية منها اسم المستخدم طالب الشهادة واسم سلطة المصادقة Certification Authority المانحة لها وتاريخ صلاحية الشهادة الممنوحة.

إن وظيفة هذه الشهادات تشبه بطاقة الهوية التي تصدرها جهة ثالثة مستقلة ومحايدة، لتعرّف عن الشخص الذي يحملها، وعن سلطاته أو اهليته أو احياناً عن مؤهلاته المهنية الخ..، وتصادق على توقيعه ألكترونياً وعلى المبادلات والصفقات التي يجريها عبر شبكة الإنترنت.

ان تدخّل الشخص الضامن في الصفقات الإلكترونية وعمليات النقل، وتبادل الرسائل بواسطة شبكة الإنترنت، من شأنه أن يخدم نظام الإثبات القانوني بفاعلية. لأن حضور الشخص الثالث(كالشاهد)،

[90]Colloque du 13 avril 2010 à la première chambre de la cour d’appel de Paris

يحسن من نوعية الإثبات، وفي إدارة مسائله والتحكم بها. ما يسمح بتعزيز فاعلية هذا الإثبات، هو التدخل المستقل والمحايد من الشخص الثالث: أي حياده عن القائمين بالصفقة موضوع المصادقة، وعدم تدخله في مضمون الرسائل المتبادلة من قبلهم.

وبالتالي يمكن القول أن مصادقة الشخص الثالث هي في الحقيقية مهنة جديدة ظهرت نتيجة ظهور شبكة الإنترنت، وترمي إلى تأمين أمن الصفقات الإلكترونية المبرمة بواسطة هذه الشبكة واثباته[91].

ويقول في هذا المجال الفقيه الفرنسي "Bensoussan" إأن وظيفة الشخص الثالث، الذي يضمن هوية شخص معين وأهليته، تشبه وظيفة الكاتب بالعدل. ولهذا السبب يستخدم البعض عبارة الكاتب بالعدل الإلكتروني Notaire Electronique لتسمية الشخص الثالث المصادق[92].

انطلاقا مما تقدم، يمكن القول إن مهنة مصادقة الشخص الثالث، حديثة العهد، تتطلب إيجاد نظام قانوني تشريعي خاص بها، يحدد الوضعية القانونية للمصادقة أو للمؤسسات والشركات التي تقدم الخدمات المماثلة، ومنح الشهادات الإلكترونية التي يصدرونها درجة معينة من المصداقية والقوة الثبوتية وفق معايير نموذجية تتوافق مع المعايير العلمية المعتمدة وتراعي التطور التكنولوجي المستمر.

ولقد أقدم المشرع اللبناني، ولو بخطوة متأخرة، على تناول هذا الموضوع في الفصل الثالث من القانون ٨١، وذكر في المادة ١٥ منه أن "مقدم خدمات المصادقة" له دور أساسي في تعزيز موثوقية الدليل من خلال تأمين عملية حماية الدليل الرقمي[93]. بالإضافة إلى إضفاء نوع من القوة الثبوتية

---

[91] عيسى، **التنظيم القانوني لشبكة الإنترنت**، مرجع سابق صادر ص ٢٠٥.

[92] Bensoussan (Alain), un nouveau métier, le tier certificateur, se profile sur l'internet, online Journal 15 dec 1995.

[93] **المادة ١٥ من القانون ٨١ تاريخ ١٠-١٠-٢٠١٨**: تهدف وسائل الحماية التي تطبق على الكتابات والتواقيع الإلكترونية إلى تعزيز موثوقيتها.تكون وظيفة وسائل الحماية التحقق من هوية واضع السند و/أو اعطاء تاريخ صحيح له و/أو ضمان سلامة بنوده وتأمين حفظه. يؤمن هذه الوظائف أو كل منها مقدم خدمات مصادقة أو عدة مقدمين،

على التوقيع الإلكتروني، الذي يعتبر من الأدلة الرقمية الأكثر تداولاً، إذا ما تمت المصادقة عليه من قبل مقدم خدمات مصادقة معتمد لدى القضاء.[94]

ومن ثم جرى تفصيل شروط اعتماد "مقدمي خدمات المصادقة" في الفصل الرابع من القانون. ولكن حتى الآن لا يزال هذا الموضوع حديثًا جدًا في لبنان، ولا يوجد حتى الآن أي مقدم لهذه الخدمات.

أما بالنسبة لما سبق وذكرناه من موثوقية نظام المعلومات والتشفير والبصمة الرقمية للدليل منذ لحظة جمعه، وحتى عرضه أمام المحكمة، فما زال هناك نقص كبير في التشريع اللبناني.

"ورغم كل النقاشات والنقد الذي دار حول قضية المقدم "سوزان الحاج" والمقرصن "غبش" والتسجيلات الصوتية والمحادثات عبر الواتساب التي عرضت، لم يتناول أحد مدى صحة هذه الأدلة وموثوقية النظام المعلوماتي الذي استخرجت منه".

وإن ما يؤكد ذلك أيضًا هو انه وبعد توقيف الممثل زياد عيتاني من قبل جهاز أمن الدولة، لم يتم التأكد من صحة ونزاهة الأدلة الرقمية المقدمة ضده، وهي عبارة عن رسائل تم تبادلها عبر الفايسبوك بينه وبين حساب آخر ظُنّ أنه إسرائيلي ولم يتم التأكد من صحة ال IP التي تبين في ما بعد أنها مزيفة وليست صحيحة. وأن كل هذه المحادثات كانت غير موثوق بها كدليل رقمي. فتحول الممثل زياد عيتاني من عميل محتمل إلى بطل وطني جرى استهدافعه عن طريق الخطأ لتشابه اسمه مع اسم صحافي.

يسلمون عند إنجازها شهادة مصادقة إلى صاحبة الصفة. يمكن أن تؤمن هذه الوظائف أو كل منها بواسطة تقنيات اخرى.

[94] **المادة ١٧ من القانون نفسه:** عندما ينشأ التوقيع الإلكتروني ويُصادق عليه وفق إجراءات يقدمها مقدم خدمات مصادقة معتمد، يعتبر مستوفياً للشروط المنصوص عليها في المادة ٩ من هذا القانون، ويتمتع بقرينة الموثوقية حتى إثبات العكس.

وهذا إن دلّ على شيء، فهو يدل على أنه مازالت بعض الأجهزة الأمنية والنيابة العامة (الاستئنافية والعسكرية) غير قادرة على التأكد من صحة وموثوقية الدليل الرقمي.

والأخطر من ذلك هو عدم قدرة القاضي على تكوين القناعة الكافية، ليتخذ القرار المناسب بل يتكل على ما ينقله له الضابط العدلي.

انطلاقاً من هنا نعالج في المبحث الثاني تأثير الدليل الرقمي على سلطة القاضي التقديرية، والمشاكل التي يواجهها النظام القضائي اللبناني في هذا المجال.

المبحث الثاني : تأثير الدليل الرقمي على سلطة القاضي التقديرية

تشكل سلطة القاضي التقديرية العامل الأهم في إصدار الأحكام في القضايا الجزائية، وإحقاق الحق والعدالة، فبعد أن يتم عرض الوقائع والحيثيات كافة ودراسة الأدلة المقدمة من الأطراف في الدعوى، يتكوّن لدى القاضي نظرة تقديرية يرى في تنفيذها احقاقاً للحق والعدل، فقد يصدر قاضي التحقيق مذكرة توقيف، إذا اقتنع بوجود جرم أو مسؤولية جزائية، أو يمنع المحاكمة في الحالة العكسية، وقد يصدر القاضي المنفرد أو محكمة الجنايات الحكم بالإدانة أو البراءة.

ولتكوين القناعة الكافية يرتكز القاضي على طرق إثبات عدة، منها ما هو مباشر، ومنها ما هو غير مباشر:

الإثبات المباشر

كثيرة هي طرق الإثبات المباشرة، وقد تناولتها المادة ١٧٩ من قانون أصول المحاكمات الجزائية، مع الإصرار على ضرورة تكوين قناعة القاضي، من خلال أدلة توفرت لديه، شرط وضعها موضع مناقشة علنية أثناء الجلسة. ولعل أهم طرق الإثبات المباشر هو الاعتراف والشهادة، إذ من النادر أن تثبت الجريمة بالطريقة الكتابية.

ويليها الخبرة، أي أخذ القاضي برأي وتقارير أصحاب الخبرة في مجال معين، وهنا دور القطاع الخاص وذوي الخبرة التقنية عندما نكون أمام جمع الدليل الرقمي، وقد سبق وتحدثنا عن ذلك في بداية البحث.

وفي النهاية يأتي دور معلومات القاضي الشخصية، التي على ضوئها يبني قناعته، وهنا لا بُدّ من التوسع قليلا نظرًا لأهمية الموضوع في العالم الرقمي:

- معلومات يحصل عليها بصفة خاصة، أي مدى إلمام القاضي بالعالم الرقمي ولغة الاتصالات الإلكترونية والحاسوب.

- معلومات يحصل عليها بصفته القضائية، ويقصد بذلك مشاهدات القاضي أثناء انتقاله إلى محل الجرم أو تفتيشه المنازل وضبط المواد الجرمية. إذا كان للقاضي المدني دور سلبي بما يقدمه الفرقاء من ادعاءات واثباتات، فله العكس في النطاق الجزائي. فعلى عاتقه يقع الكشف عن الحقيقة، ونرى ذلك بشكل واضح في الصلاحيات الواسعة التي منحت له في الجريمة المشهودة، مثال على ذلك وجوب انتقال النائب العام إلى مسرح الجريمة، وتنظيم المحاضر اللّازمة، وجمع الأدلة واستجواب المشتبه فيهم... ولقاضي التحقيق أيضًا في مثل هذه الحالات، مباشرة المعاملات نفسها التي هي من صلاحيات النائب العام، وله حق الانتقال سواء كانت الجريمة مشهودة أم غير مشهودة، وسواء كانت جنحة أم جناية.

اضف إلى ذلك المعلومات التي يحصل عليها القاضي من خلال التحقيقات الإضافية مستعيناً بأهل الخبرة[95]، والتي سبق وتحدثنا عنها سابقاً.

الإثبات غير المباشر أو ما يسمى بالقرائن:

و هو استنتاج واقعة غير معروفة من وقائع أخرى معروفة مرتبطة بها ارتباطاً وثيقاً: منها ما هو **قانوني** مثل "مرور الزمن" قرينة على الإيفاء وحيازة المنقول يشكل سند ملكية له، ومنها ما هو **تقديري** وهي القرائن غير القانونية أو الأمور التي تترك للقاضي، ويستخلصها من ظروف كل قضية وملابساتها، ويصحّ الاستناد إليها في تعزيز الأدلة الأخرى القائمة بالدعوى، مثل توجيه المتهم التهديدات إلى المجني عليه قبل الحادث، أو مثلا شراء سلاح قبل وقت قريب من الجرم، أو دخول الإرهابي إلى مواقع رقمية على الإنترنت تعلم كيفية صنع عبوات غير نظامية معدة للتفجير الخ....

و من هنا نرى أن اقتناع القاضي وقدرته على استنتاج الوقائع والتعرف إلى الأدلة الرقمية يحتاج إلمامًا بالعالم الرقمي، كون الإثبات في القضايا الجزائية أمرًا حرًا وواسعًا، تلعب فيه قناعة القاضي الدور الأهم، وليس كالقضاء المدني، حيث الإثبات محدد وواضح حسب القوانين.

---

[95] نصر (فيلومين)،أصول المحاكمات الجزائية، دراسة مقارنة وتحليل، الطبعة الأولى ٢٠١٣ ، المؤسسة الحديثة للكتاب ص ٤٨٢.

نعرض في ما يلي أهمية إلمام القاضي بالعالم الرقمي أثناء دراسة الأدلة الرقمية، وضرورة العمل على إنشاء هيئة قضائية متخصصة في العالم الرقمي.

البند الأول: مدى إلمام القاضي بالعالم الرقمي

للعالم الرقمي لغة تقنية خاصة ومعقدة بعض الشيء، لذلك لا بُدّ للضابطة العدلية والجهاز القضائي من الإلمام بها والاطلاع عليها، من أجل فهم ماهيّة الدليل الرقمي وكيفية التعامل معه. وإن عدم إلمام المحقق والقاضي بهذه اللغة، قد يشكل عقبة أمام إحقاق الحق. إذ يصبح الدور الأهم في يد أصحاب الخبرة فقط.

لا نرى هذه العقبة عند الضابطة العدلية وخاصةً قوى الأمن الداخلي إذ أصبح هناك مكاتب متخصّصة في العالم الرقمي وجرائم المعلوماتية، مشكلة من ضباط ورتباء أصحاب اختصاص.

ولكن عند الحاجة إلى أَخذ إشارة النيابة العامة أو عند وصول الدعوة إلى التحقيق الابتدائي، تبدأ هذه المشكلة بالتبلور أكثر فأكثر، إذ إن أغلب الجهاز القضائي، وخاصةً القديم منه، ليس على اضطلاع كاف بالعالم الرقمي واللغة التقنية الرقمية. وهذا الموضوع يحد من قدرة القاضي على الاقتناع بما يصل إليه من أدلة رقمية، كونه ليس على علمٍ كافٍ بالعالم الرقمي، ويصبح من دون أن يعلم، مرتبطًا بما يمليه عليه صاحب الاختصاص(ضابطًا عدليًا أم خبيرًا تقنيًا) الذي جمع الدليل الرقمي للجريمة أو قام بتحليله.

وما يزيد الموضوع خطورة، أنه بهذه الطريقة يصبح الضابط العدلي المعني بالتحقيق وبالأدلة الرقمية هو المحقق والحكَم في الوقت نفسه وذلك بسب ثقته بان القاضي، أكان نائباً عاماً استئنافياً ام قاضي تحقيق، أم على قوس المحكمة، لن يتأكد من موثوقية نزاهة الدليل الرقمي المقدم. وهذا ما يتنافى مع مبدأ فصل سلطة التحقيق عن سلطة المحاكمة، لضمان صدور حكم موضوعي، ولتحقيق العدالة. وبصبح بذلك الضابط العدلي قادرًا على "فبكرة" أدلة رقمية قد تدين أشخاصًا بريئين تماماً.

من هنا لا بُدّ للقاضي من أن يخضع لدورات تدريبية في العالم الرقمي ويحصل على الحد الأدنى من الاطلاع على مكونات الحاسوب ونظام الإنترنت، وماهية البروتوكول(IP)، وحتى التعرف ودراسة

بعض التعابير، التي تخص جرائم المعلوماتية مثل ال PISHING[96]، HACKING[97] وغيرها، وفهم كيفية استخدام العالم الرقمي في تحديد المكان الجغرافي للمشتبه به، أو حتى اعتراض حزمات المعلومات، وكيفية ضمان سلامة الدليل الرقمي بعد جمعه، من أجل تعزيز قدرته على الاقتناع بما يعرض أمامه من أدلة، وإصدار الأحكام العادلة.

نعرض بعض حيثيات القرار الصادر عن محكمة التمييز[٩٨]، الغرفة السابعة عام ٢٠١٣ لأنه يلقي الضوء على أهمية اقتناع القاضي بالدليل الرقمي المقدَّم من أجل إصدار الحكم:

انضم المدعو "مسعود شعيب" الى دعوة إساءة الأمانة المقدمة من والدته ضد المدعي عليه "رودي سمعان" مرفقًا بادعائه تسجيل مكالمة هاتفية جرت بينه وبين المدعى عليه بعد تخلية سبيل هذا الاخير، يستدل منها اعتراف المدعى عليه باستلام مبلغ ستين الف دولار اميركي واشتراطه لرده أو رد جزء منه، رجوع والدة المدعي عن دعوى إساءة الأمانة المقدمة أمام القاضي المنفرد الجزائي في بعبدا الذي بدوره اصدر حكمًا قضى بإدانة المدعى عليه.

وبنتيجة الاستئنافين المقدمين من المدعي والمدعى عليه، أصدرت محكمة استئناف الجنح في المتن قرارًا خلصت فيه إالى تصديق الحكم الإبتدائي.

---

96 Phishing التصيد الاحتيالي هو محاولة للحصول على معلومات حساسة مثل أسماء المستخدمين وكلمات المرور وتفاصيل بطاقة الائتمان والأموال) غالبًا لأسباب ضارة ، وذلك بالتنكر ككيان جدير بالثقة في اتصال إلكتروني

97 Hacking : هاكر أو قرصان أو مخترق (بالإنجليزية: Hacker) هم مبرمجون محترفون في مجالات الحاسوب يوصف بأسود(Black Hat Hacker) إذا كان مخرب وأبيض (أو أخلاقي) (White Hat Hacker) إذا كان يساعد على أمان الشبكة والآمن المعلوماتي و رمادي أو ما يسمى (Gray hay hacker) أو "المتلوّن" وهو شخص غامض غير محدد اتجاهه لأنه يقف في منطقة حدودية بين الهاكرين الأسود والأبيض. ويمكن في بعض الحالات أن يقوم بالمساعدة وفي حالات أخرى يكون هدفه ضحية معينة، عمومًا كلمة تصف الشخص المختص والمتمكن من مهارات في مجال الحاسوب وأمن المعلوماتية. وأطلقت كلمة هاكر أساسا على مجموعة من المبرمجين الأذكياء الذين كانوا يتحدون الأنظمة المختلفة ويحاولون اقتحامها.

٩٨ محكمة التمييز الجزائية، الغرفة السابعة، قرار رقم ٢٠١٣/١٠٠،"رودي سلمان/الحق العام و"صباح البدوي".

والجدير ذكره أن محكمة التمييز اعتبرت ان هذا الدليل المقدَّم (التسجيل الصوتي) ينزل منزلة الإقرار غير القضائي خاصةً وأن المدعى عليه استنبط لجوءَ المتصل الى تسجيل المكالمة وارتضى رغم ذلك، ولأن الأقوال والإدلاءات تدلّ دلالة كافية على الشخص الصادرة عنه هذه التصريحات، وأن الإقرار غير القضائي المحكى عنه وبالشكل الوارد فيه يشكل حجة ضد المدعى عليه يكون بالتالي الحكم الإبتدائي في محله القانوني.

هذا القرار إن دلَّ على شيء، فهو يدلّ على مدى أهمية اقتناع القاضي بالدليل الرقمي المقدَّم، ففي هذه الحالة اقتنعت محكمة التمييز بصحة التسجيل الصوتي وبعودته الى المدعى عليه دون اللجوء الى الخبراء التقنيين، وهذا ما ساهم في إصدار حكمٍ عادلٍ.

البند الثاني: التدريب المتواصل للقضاة والضابطة العدلية

في مكافحة جرائم تكنولوجيا المعلومات والاتصالات وجمع الدليل الرقمي، لا بُدّ من وضع خطة جنائية سليمة، تستند إلى تدريب أجهزة الضابطة العدلية والقضاة وتجهيزهم للتعامل مع الأدلة الرقمية، وقد تنبهت الدول إلى أهمية هذا التدريب، وإعداد كوادر شرطية على درجة عالية من الكفاءة والمهارة، للتعامل مع هذه الأنماط الإجرامية المستحدثة.

وهذا يعتمد بالضرورة على العملية التدريبية، وهي المدخل أو الطريق السليم للوصول إلى تنمية القدرات والمهارات، ورفع مستوى الأداء، لذا أصبح من الضروري تطوير العملية التدريبية بما يتواكب مع مستجدات العصر، وبما يلبّي الاحتياجات الأمنية الحالية والمستقبلية كافة ويُسهم بفعالية في خلق كفاءات بشرية قادرة على الإمساك بزمام المبادرة في منظومة أمنية متكاملة قادرة على التعامل مع الدليل الرقمي وتعقيداته، من دون تجاوز الحدود والشرعية، وقادرة على تحليل ما يقابلها من مشكلات، ووضع رؤى وتصورات صحيحة وسليمة لحلها.

ولهذا يجب إعداد الضابطة العدلية والقضاة سوياً، وتدريبهم على التعاطي مع جرائم الحاسب الآلي والإنترنت، لأنهم يواجهون أنشطة إجرامية معقدة، تنفَذ بطريقة دقيقة وذكية من الكبار والقاصرين على حد سواء.

وليس بالضرورة أن يكون المحقق خبيراً في الحاسب الآلي، لكن لا بُدّ له من الإلمام ببعض المسائل الأولية، التي تمكنه من التفاهم مع خبراء الحاسب الآلي، وحسن استغلالها في كشف الجرائم وجمع الأدلة، كما أنه من الضروري أن يكون المحقق ملمّاً بالإجراءات الاحتياطية التي ينبغي اتخاذها على مسرح الجريمة، في جرائم الحاسب الآلي، والتدابير اللّازمة لتأمين الأدلة ومعلوماتها الممغنطة بصورة علمية وسليمة.

ولقد عمدت المنظمات الحكومية ومنظمات الشرطة في بعض الدول إلى تدريب رجالها، وذلك بإعداد دورات تخصصية متتابعة ومستمرة لهم في هذا المجال، ومن بين تلك الدول: الولايات المتحدة الأمريكية، التي نظّمت تلك الدورات المتخصصة، مدة كل منها أربعة أسابيع، وذلك من أجل تزويد محققي الشرطة والقضاة والعاملين في إدارات العدالة الجزائية بمعارف ومهارات هدفها برمجة الحاسوب وتشغيله [99].

في لبنان، وفي مبادرة فريدة وجديدة تم اطلاق أول دائرة تحقيق إلكتروني في قصر عدل طرابلس وتخلية سبيل ٢٥ موقوفاً عن الهيئة الإتهامية و٩ موقوفين عن جنايات الشمال، استناداً الى التعاميم الصادرةِ عن رئيس مجلس القضاء الأعلى، ووزيرة العدل، ومدعي عام التمييز المتعلقة بتسهيل تقديم طلبات إخلاء سبيل الموقوفين، والتوقيف الاحتياطي والاستجواب الالكتروني، وبتنسيقٍ وتعاون فيما بين الرئيس الأول لمحاكم الإستئناف في الشمال ونقيب المحامين في طرابلس والشمال وقاضي التحقيق الأول في الشمال، ورؤوساء محاكم جنايات الشمال وإستئناف الجزاء، والنيابة العامة، وقضاة الجزاء المنفردين،

ليبدأ العمل بها بداية شهر نيسان ٢٠٢٠، بالتعاون مع غرفة الـ "Call Center" في نقابة المحامين، بحيث خصِّص بريد إلكتروني لكلٍّ منهما، لتسهيل إرسال وتلقي طلبات تخلية السبيل وفرزها، ستقوم لجنة السجون بتلقي طلبات تخلية السبيل عبر الـ "Call Center" أو عبر الفاكس، من أماكن التوقيف والإحتجاز في الشمال، أو عبر الوكلاء المحامين، ويقوم الموظفون بإعادة فرزها وتسليمها للقضاة المختصين عبر البريد الإلكتروني.

---

[99] رستم (هشام)، الجرائم المعلوماتية، أصول التحقيق الجزائي الفني وآلية التدريب التخصصي للمحققين، مجلة الأمن والقانون، كلية الشرطة دبي، العدد الثاني، السنة السابعة ١٩٩٩ ص٣٠ .

كما اعتُمدت تجربة الإستجواب بتقنية الصوت والصورة عبر برنامج" zoom"، الذي يقوم بتسجيل الإستجواب مباشرةً، والذي سيتم إستخدامه لإستجواب الموقوفين وإعتماده لدى جميع مراكز التوقيف في الشمال، كما يستطيع المحامي عبر التطبيق نفسه المشاركة، أو الحضور لدى قاضي التحقيق أو في مركز التوقيف أثناء الإستجواب عبر البرنامج[100].

وفي الخلاصة، إن تنفيذ الضابطة العدلية إجراءات رفع الدليل الرقمي بشكل يضمن سلامته ونزاهته والحفاظ عليه وتخزينه بطريقة آمنة، من شأنه أن يزيد من قوته الثبوتية، وقدرته على إقناع القاضي الذي بدوره، عليه ان يكون على اطلاع كافٍ على العالم الرقمي وتعقيداته من خلال متابعة دورات تدريبية مستمرة في هذا المجال؛ وهذا ما يضع لبنان أمام تحديات وطنية داخلية كبيرة. ولكن الصعوبات لا تقف على الصعيد الداخلي فقط، بل تتعداه ايضاً إلى العالم الدولي حيث لا بدّ من اتباع أصول محددة في التعاون مع الدول من أجل جمع الأدلة الرقمية المخزنة خارج الإقليم اللبناني، وهنا تصبح الأمور أكثر تعقيدًا.

---

[100]منشور على موقع/Al Majalla Al Kadaiyatالمجلة القضائيةhttps://www.facebook.com/alkadaiyat
(last revision 31/3/2020) March 26 at 8:53 PM

الفصل الثاني: التعاون الدولي أساس لجمع الدليل الرقمي

تنبع حاجة لبنان إلى تفعيل التعاون مع الدول الأخرى في موضوع رفع دليل الرقمي، من التطور الإلكتروني والتقني في هذه الدول وأهمها للولايات المتحدة الأميركية ودول الاتحاد الأوروبي. فالأولى تتلقى بشكل كبير طلبات مساعدة قانونية من أغلبية دول العالم إذ إن إدارة أكثرية الشركات التي تزود العالم بخدمة الإنترنت وتطبيقات وسائل التواصل الاجتماعي تتمركز فيها، والثانية (دول الاتحاد الأوروبي) هي الأنجح في وضع الأطر القانونية لهذا التعاون الدولي الملح. ولقد تجلى ذلك في إتفاقية بودابست عام٢٠٠١ لجرائم المعلوماتية.

إن العالم الرقمي لا حدود له، فهو يغطي الدول كافة ، وان لم يتم تنظيم إطار العمل والتعاون في ما بينها، يمكن للمجرمين الإلكترونيين، أن يستغلوا الحدود الجغرافية والفوضى في تبادل المعلومات الرقمية، والتعاون الدولي في مكافحة الجرائم، من أجل التهرب من العقاب والعدالة، وبالأخص المنظمات الإرهابية والاتجار بالبشر وغيرها.

من هنا لا بُدّ من معرفة صلاحيات الدول، في تطبيق قوانينها على مثل هذه الجرائم، سيما وأن عناصرها قد يكونون منتشرين في أكثر من دولة. وفي حال الإيجاب، ينبغي اعتماد أفضل وسائل ممكنة لتوفير المساعدة القانونية المتبادلة بين الدول، من أجل عدم ضياع الأدلة الرقمية، ولا بُدّ أن يتم ذلك من خلال أطر واضحة ومحددة في اتفاقيات دولية عصرية، مثل إتفاقية "بودابست للجريمة" الإلكترونية التي أقرها مجلس الدول الأوروبية عام٢٠٠١.

<u>المبحث الأول :</u> تحديد الاختصاص في جرائم المعلوماتية

يقصد بالاختصاص، "السلطة التي يقررها المشرع للقضاء، للنظر في دعاوى معينة حددها القانون"[101] والاختصاص، على نوعين: الأول هو تطبيق سلطان الشريعة الجزائية على الأرض اللبنانية، أي الحالات التي يكون فيها القانون الجزائي في دولة ما مختصاً بنظر دعاوى معينة، والثاني الاختصاص الداخلي ويقصد به، توزيع الدعاوى الجزائية وفق معايير محددة داخل الدولة، بعد أن ينعقد لها الاختصاص الدولي.

إنّ مسألة الاختصاص القضائي تسهُل عند الحديث عن الجرائم التقليدية أو العادية. أما أمام تلك التي ترتكب عبر العالم الرقمي الافتراضي، فهي تشكّل مشكلة معاصرة تواجه القضاء الجزائي، إذ إن المشكلة الأساسية لجرائم تكنولوجيا المعلومات والاتصالات، تكمن في كونها لا تعرف حدودًا جغرافية محسوسة، بل يكون مسرحها الفضاء السيبراني وعالم الإنترنت.

وبالتالي وأمام هذا التطور التقني الذي لا يمكن للتشريع أن يواكبه بالشكل المطلوب، لا بُدّ لنا أن نلجأ إلى تفسير النصوص الحالية، وتطبيق المبادئ ذاتها المعمول بها لحل مشكلة الاختصاص الجزائي في الجرائم التقليدية:

- مبدأ إقليمية القانون الجزائي، أو ما يعرف بالصلاحية الإقليمية أي تطبيق القانون على كل جريمة تحدث داخل إقليم الدولة.

و الاستعانة بالمبادئ الأخرى التي تسمح بامتداد تطبيق القانون خارج إقليم الدولة مثل:

- مبدأ عينية النص الجزائي، أو الصلاحية الذاتية، أي تطبيق القانون على كل الجرائم التي تمس مصالح الدولة وهيبتها أيا كانت جنسية مرتكبها.

---

[101] عبد الرؤوف الخنّ (محمد) جريمة الاحتيال عبر الإنترنت، الأحكام الموضوعية والأحكام الإجرائية، الطبعة الأولى ٢٠١١، منشورات الحلبي الحقوقية ص ١٩٧

- مبدأ شخصية النص الجزائي، أي تطبيق النص الجزائي على كل جريمة يرتكبها من يحمل جنسية الدولة.

- مبدأ عالمية النص الجزائي، أو الصلاحية العالمية أو الشاملة، أي تطبيق النص الجزائي على كل جريمة مرتكبة خارج إقليم الدولة، إذا كان الجاني أجنبيًا ومقيمًا على إقليمها، ولم يكن قد طُلب تسليمه إلى إحدى الدول لمحاكمته أو قُبِل الطلب.

البند الأول: الصلاحية المكانية للقانون الجزائي اللبناني في الجرائم الرقمية

يقصد بمبدأ إقليمية القانون الجزائي، أن يطبّق القانون الجزائي لدولة على كل جريمة ترتكب على اقليم هذه الدولة، سواء كان الجاني يحمل جنسية هذه الدولة، أو يحمل جنسية دولة أجنبية، وسواء أكان المجني عليه مواطناً أم أجنبياً.

ويستند هذا المبدأ إلى عدة مبررات، منها فكرة سيادة الدولة على إقليمها، إذ إن تطبيق القانون الجزائي إقليمياً هو من أهم مظاهر السيادة، فقانونُها الجزائي هو الذي يضمن حماية الحقوق الدستورية والقانونية على أراضيها.

إضافة إلى أَن قضاء مكان ارتكاب الجريمة يكون قادرًا على جمع الأدلة اللازمة والإحاطة بجميع ظروفها بسرعة وفاعلية أكثر، كما أن محاكمة الجاني في مكان ارتكاب الجريمة يحقق الردع العام، ويقضي على الاضطراب الاجتماعي الذي أحدثته الجريمة.

ولقد حدد قانون العقوبات الإقليم اللبناني في المادتين١٦و١٧[102] بحيث قسمت إلى أربعة أقاليم: الإقليم البري وهو المساحة من الكرة الأرضية التي تقع ضمن الحدود اللبنانية المعينة سياسياً

---

[102] المادة ١٦ من قانون العقوبات اللبناني :تشمل الأرض اللبنانية طبقة الهواء التي تغطيها، أي الإقليم الجوي.

المادة ١٧ من قانون العقوبات اللبناني معدلة وفقا للقانون ٥١٣ تاريخ ١٩٩٦/٦/٦ يكون في حكم الأرض اللبنانية، لأجل تطبيق الشريعة الجزائية: من الشاطئ ابتداء من أدنى مستوى الجزر. ١ –البحر الإقليمي إلى مسافة عشرين كيلو مترا ٢ –المدى الجوي الذي يغطي البحر الإقليمي. ٣ –السفن والمركبات الهوائية اللبنانية. ٤ –الأرض الأجنبية التي يحتلها جيش لبناني، إذا كانت الجرائم المقترفة تنال من سلامة الجيش أو من مصالحه. ٥ –المنطقة المتاخمة

ودولياً: و شمل سطح الأرض وما في باطنها، كما يشمل البحيرات والأنهار الداخلية والأجزاء التابعة للدولة من الأنهار الدولية والبحار المغلقة.

الإقليم البحري وهو البحر المتصل بالأرض اللبنانية حتى مسافة عشرين كيلو متراً والإقليم الجوي أي طبقات الهواء التي تغطي الإقليمين البري والبحري إلى ما لا نهاية والإقليم الممتد أو الاعتباري:

١. السفن والمركبات الهوائية اللبنانية أينما وجدت ،سواء كانت ملكاً للدولة أم للأفراد، ما دامت مسجلة في لبنان.

٢. الأرض الأجنبية التي يحتلها الجيش اللبناني إذا كانت الجرائم المقترفة عليها تنال من سلامة الجيش أو من مصالحه.

متى تعتبر الجريمة الإلكترونية مقترفة على الأرض اللبنانية ؟ و ما هو المقصود بالإقليم اللبناني في جرائم تكنولوجيا المعلومات والاتصالات ؟

تَنصّ المادة ١٥ من قانون العقوبات اللبناني على أن الجريمة تعد مقترفة على الأرض اللبنانية في حالتين:

- إذا تم على هذه الأرض أحد العناصر التي تؤلف الجريمة، أو فعل من أفعال جريمة غير متجزئة أو فعل اشتراك أصلي أو فرعي.
- إذا حصلت النتيجة على هذه الأرض أو كان متوقعا حصولها عليها.

والمنطقة الاقتصادية المانعة والجرف القاري التابعة للبنان والمنصات الثابتة في هذا الجرف القاري، تطبيقا لأحكام اتفاقية الأمم المتحدة لقانون البحار الموقعة بتاريخ مونتيغو باي (الجامابيك) في ١٩٨٢/١٢/١٠. الذي أجيز للحكومة الانضمام إليها بموجب القانون رقم ٢٩ تاريخ ١٩٩٤/٢/٢٢.

من الملاحظ أن المشرع اللبناني أراد أن يوسع من صلاحيات الدولة الإقليمية، ولقد استخدم في هذا التوسع الركن المادي (الفعل والنتيجة والرابطة السببية) كمعيار لتحديد ما إذا كانت الجريمة قد وقعت على الأراضي اللبنانية، إذ لا يمكن الاكتفاء بالركن المعنوي فقط[103].

وبالتالي فلا مشكلة إذا كانت جميع عناصر الجريمة قد وقعت في الأراضي اللبنانية، مثل قيام شخص مقيم في لبنان باختراق النظام المعلوماتي لأحد المصارف في لبنان وتحويل أرصدة بعض الحسابات إلى حسابه المصرفي اللبناني، فهنا جميع عناصر الاحتيال تكون قد وقعت على الأراضي اللبنانية.

ولكن تطبيق مبدأ الإقليمية ليس دائمًا بهذه السهولة كون عناصر أغلب جرائم المعلوماتية تكون موزعة بين الدول. سنأخذ في ما يلي جريمة الاحتيال كمثال، نظرًا لكثرة شيوع هذه الجريمة في أيامنا هذه.

متى يعقد الاختصاص الإقليمي للقضاء اللبناني:

١- إذا تم على الأرض اللبنانية أحد عناصر الجريمة: مثل قيام شخص موجود في لبنان بإنشاء موقع للاحتيال عبر الإنترنت، سواء كان الموقع مستضافاً على مخدم لبناني أو أجنبي ثم يقع ضحية هذا الموقع شخص مقيم في فرنسا.

٢- إذا تم على الأرض اللبنانية فعل من أفعال جريمة غير مجزّأة: (جريمة مستمرة ومتتابعة أم جريمة العادة) حيث يوجد وحدة في الإرادة الجريمة، وحدة الحق المعتدى عليه ووحدة الغرض مثال قيام شخص موجود في أوروبا بالاحتيال عدة مرات عبر البريد الإلكتروني على شخص مقيم خارج الأراضي اللبنانية من أجل الاستيلاء على مبالغ مالية إذا ثبت أنه تواجد في إحدى المرّات ولو مرة واحدة على الأراضي اللبنانية.

---

[103] عبد الرؤوف الخنّ (محمد) جريمة الاحتيال عبر الإنترنت ، الأحكام الموضوعية والأحكام الإجرائية، الطبعة الأولى ٢٠١١، منشورات الحلبي الحقوقية ص ٢١٢

٣- اذ وقع على على الأراضي اللبنانية فعل اشتراك أصلي أو فرعي: كما لو اشترك شخص موجود في لبنان بعملية اختراق لنظام معلوماتي عبر الإنترنت عائد لأحد المصارف الأميركية بقصد الاحتيال مع شخص آخر موجود في اليابان (اشتراك أصلي) ام إعطاء الإرشادات والمعلومات اللّازمة(إشتراك فرعي).

٤- إذا حصلت النتيجة الجرمية على الأرض اللبنانية أو كان متوقعًا حصولها فيها (أي المحاولة الجرمية) مثال قيام شخص موجود في مصر بالاحتيال عبر الإنترنت على شخص موجود في لبنان(حصول النتيجة) أم استخدام بطاقة الائتمان الخاصة للبناني من دون علمه الّا أنَّ السحب لم يصل لأسباب خارجة عن إرادة الجاني (محاولة).

من خلال ما سبق، يظهر جليًا الارتكاز في تحديد الاختصاص الإقليمي على وجود الجاني أو نظام الحاسوب العائد له داخل الأراضي اللبنانية أثناء ارتكاب الجريمة، قياساً الى الجريمة التقليدية، مع الأخذ بعين الاعتبار، الاستثناءات على تطبيق الشريعة اللبنانية التي نصت عليها المادتان ١٨ و٢٢ من قانون العقوبات.[104]

وهناك تساؤل يتبادر إلى الأذهان أثناء دراسة انعقاد الاختصاص الإقليمي في جرائم المعلوماتية:

---

[104] **المادة ١٨ من قانون العقوبات** :لا تطبق الشريعة اللبنانية:

١ –في الإقليم الجوي اللبناني، على الجرائم المقترفة على متن مركبة هوائية أجنبية إذا لم تتجاوز الجريمة شفير المركبة. على أن الجرائم التي لا تجاوز شفير المركبة الهوائية تخضع للشريعة اللبنانية إذا كان الفاعل أو المجنى عليه لبنانيا . ً ، أو إذا حطت المركبة الهوائية في لبنان بعد اقتراف الجريمة.

٢ –في البحر الإقليمي اللبناني أو في المدى الجوي الذي يغطيه، على الجرائم المقترفة على متن سفينة أو مركبة هوائية أجنبية إذا لم تجاوز الجريمة شفير السفينة أو المركبة الهوائية.

المادة ٢٢ لا تطبق الشريعة اللبنانية في الأرض اللبنانية على الجرائم التي يقترفها موظفو السلك الخارجي والقناصل الأجانب ما تمتعوا بالحصانة التي يخوله إياها القانون الدولي العام.

أليس من الجائز اعتبار تلك المساحة من الإنترنت الخاضعة لإدارة الدولة اللبنانية والتي تنتهي باللّاحقة "**LB.**" جزءاً من الأرض اللبنانية؟

وللإجابة عن هذا السؤال ننطلق من التحليل التالي:

١. إن المبررات المتعلقة بسيادة الدولة اللبنانية على إقليمها، والتي تدفع بالمشرع إلى اعتبار الطائرة أو السفينة اللبنانية بحكم الأرض اللبنانية، متوفرة في النطاق الرقمي اللبناني على الإنترنت، في كونه خاضعًا لإدارة الدولة اللبنانية. وبالتالي يصبح مثل الطائرة أو السفينة التي تحمل العلم اللبناني أو الجنسية اللبنانية، وتحقيق العدالة يكون أقرب وأسرع خاصةً مع سهولة وسرعة جمع الأدلة الرقمية اللازمة للإثبات.

٢. هل يجوز ارتكاب الجرائم الرقمية على النطاق اللبناني "**LB.**" من دون أن يطالها العقاب حسب القانون الجزائي اللبناني؟ مثال: إذا أنشأت شركة إيطالية موقعاً ألكترونياً لها على النطاق اللبناني، ثم قامت عبر هذا الموقع بالاحتيال، أو استغلال المعلومات الشخصية لبعض الاشخاص الموجودين في اسبانيا، لا يمكن تطبيق الصلاحية الإقليمية للدولة اللبنانية لمعاقبة هذه الشركة في القوانين الحالية.

٣. مع العلم انه من الممكن التوسع في تفسير الصلاحية الذاتية للدولة اللبنانية، واعتبار أن استخدام هذا النطاق العلوي اللبناني من أجل ارتكاب الجرائم عبر الإنترنت، يشكل تهديدًا لأمن الدولة اللبنانية ويمس بمكانة الدولة اللبنانية في العالم الرقمي الاقتصادي والأمني.

وفي خطوة جيدة، خصص المشرع اللبناني القسم الرابع من القانون رقم ٨١ تاريخ ٢٠١٨/١٠/١٠ للمسألة عينها، بحيث عرّف النطاق اللبناني، وحدد كيفية إدارة وتسجيل أسماء المواقع، ضمن النطاق اللبناني من خلال هيئة وطنية لإدارة النطاقات الخاصة بلبنان.[105] كما وشدد على حفظ حقوق الغير

---

[105] **المادة ٧٩ من القانون ٨١ تاريخ ٢٠١٨/١٠/١٠** : تنشأ بموجب هذا القانون هيئة تسمى " الهيئة الوطنية لادارة النطاقات الخاصة بلبنان" (registry). تتولى الهيئة مهام ادارة وتسجيل أسماء المواقع ضمن النطاقات الخاصة

على هذا النطاق تحت طائلة المساءلة القانونية [106] وأن النزاعات حول التسميات بأسماء المواقع عبر هذا النطاق، تكون من اختصاص المحاكم اللبنانية، ويمكن اللجوء إلى التحكيم[107]، ما يدلّ على رغبة وإرادة المشرع اللبناني، بإخضاع النطاق اللبناني لسلطان القانون اللبناني، وهذا أمر لا بُدّ منه منطقياً.

أضف إلى ذلك، فان مسألة **البث** قد تشكل عاملاً أساسياً أو شرطاً مهمًا لدى العديد من الدول، من أجل انعقاد الاختصاص الإقليمي: ففي فرنسا يعد البث أحد العناصر المكونة لجريمة الاستغلال

بلبنان (.lb. لبنان. وغيرها من المواقع) بعد اجراء التحقيقات الازمة وفقا لتعرفة تتوافق مع تنمية سوق عملايات التسجيل.

تتألف الهيئة من ممثلين عن وزارة الاتصالات، وزارة الاقتصاد والتجارة، وزارة المالية، وزارة العدل، وزير الدولة لشؤون التنمية الإدارية، الهيئة الناظمة للاتصالات، اتحاد غرف التجارة والصناعة والزراعة، نقابة المحامين، وممثلين عن عدد من الجمعيات العاملة المعنية بهذا القطاع يتراوح بين ثلاثة وخمسة على أن تتم تسميتهم من قبل الهيئة المذكورة وتستبدل أي جمعية تصبح غير عاملة من قبل الهيئة.

[106] **المادة ٨١ من القانون نفسه:** يمكن تسجيل اسم الموقع وإدارته عن بعد عبر الوسائل الإكترونية.

يسجل اسم الموقع مع حفظ حقوق الغير. عند مخالفة هذه الأحكام تترتب المسؤوليات القانونية عند الاقتضاء على طالب اسم الموقع، والتي يمكن ان تؤدي إلى إلغاء أو نقل ملكية اسم الموقع الممنوح.

[107] **المادة ٨٢ من القانون نفسه:** تختص المحاكم في فصل النزاعات المتعلقة بأسماء المواقع.

لا تعتبر الهيئة طرفاً في النزاع بل تُنفذ الأحكام الصادرة في النزاعات عن المحاكم اللبنانية.

يمكن تسوية النزاعات القابلة للصلح المتعلقة بأسماء المواقع بطرق غير قضائية وتختار الجهة المخولة منح وادارة أسماء المواقع مركزاً أو أكثر لتسوية النزاعات المتعلقة بأسماء المواقع بطرق غير قضائية.

تتمتع الأحكام الصادرة عن مراكز التحكيم بالصيغة التنفيذية حكماً وتكون صالحة للتنفيذ مباشرةً عبر دوائر التنفيذ المختصة. يجب أن تتضمن شرعة تسمية أسماء المواقع على شبكة الإنترنت لائحة بأسماء المراكز والقواعد التي تعتمدها لحل النزاعات.

الجنسي للأطفال[108] وفي إيطاليا اعتبرت محكمة النقض أن جريمة القدح والذم عبر الإنترنت تعتبر محققة، ليس من الوقت الذي بُثت فيه، بل من الوقت الذي يمكن فيه قراءة الرسالة من الغير، وتعد كأنها وقعت على الأراضي الإيطالية[109].

أما القانون اللبناني فلقد اخذ بشرط البث، ولكن ليس بشكل مطلق، بل في بعض الجرائم مثل جريمة القدح والذم، ولم يشر إليه حرفياً بل استخدم تعبير العلنية ووسائل النشر، التي حددت في المادة ٢٠٩ من قانون العقوبات[110].

---

[108] **Article 227-2 du code penal** "Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Lorsque l'image ou la représentation concerne un mineur de quinze ans, ces faits sont punis même s'ils n'ont pas été commis en vue de la diffusion de cette image ou représentation.

Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peine.."

[109] عبد الرؤوف الخنّ **جريمة الاحتيال عبر الإنترنت** ، مرجع سابق ص ٢٠٨.

[110] المادة ٢٠٩ من قانون العقوبات اللبناني :–تعد وسائل نشر

١ –الأعمال والحركات إذا حصلت في محل عام أو مكان مباح للجمهور أو معرض للأنظار أو شاهدها بسبب خطأ الفاعل من لا دخل له بالفعل.

٢ –الكلام أو الصراخ سواء جهر بهما أو نقلا بالوسائل الآلية بحيث يسمعها في الحالين من لا دخل له بالفعل.

٣ –الكتابة والرسوم والصور اليدوية والشمسية والأفلام والشارات والتصاوير على اختلافها إذا عرضت في محل عام أو مكان مباح للجمهور أو معرض للأنظار أو بيعت أو عرضت للبيع أو وزعت على شخص أو أكثر.

وقد اصدرت الغرفة الثالثة في محكمة التمييز الجزائية القرار رقم ١٧٥سنة ٢٠١٦ الذي اعتبرت فيه: "ان موقع التواصل الاجتماعي الذي نشر العبارات التي تعتبر قدحًا وذمًا، هو وسيلة نشر معدة لإطلاع الجمهور، سواء في لبنان أو في منطقة جبل لبنان، بمعزل عن محل إقامة المدعى عليه سندًا للمادة من قانون٩ أصول المحاكمات الجزائية، فيكون القضاء الجزائي اللبناني مختصًا للتحقيق في الدعوى، وخاصة لجهة الاختصاص المكاني لقاضي التحقيق في جبل لبنان".

نعرض أبرز الحيثيات نظراً لأهميتها:

" حيث أن المستدعي يعيب على القرار المطعون فيه تشويه الوقائع والمضمون الواضح للمستندات المبرزة في الدعوى، في ما قضى برد الدفع بانتقاء صلاحية قضاء التحقيق في جبل لبنان للنظر في الدعوى، مستنداً إلى أن الخبر موضوع الدعوى موجود وصادر في لبنان، في حين أن المستندات والقرائن والإدلاءات تؤكد أن الخبرين مصدرهما فلسطين المحتلة، ولا علاقة للمستدعي بهما، وليست صادرة في لبنان؛ وأن العنوان الوارد في الشكوى لمحل إقامته غير صحيح، وهو المقر الأمني لحركة الجهاد الإسلامي وليس محلاً لإقامته.

وحيث أن الموقعين الإلكترونيين اللذين نشرت من خلالهما العبارات المشكو منها، يعدّان وسيلة من وسائل النشر، وأن النشر يحصل عندما يفتح الموقع الإلكتروني أمام الجمهور لتلقي ما تم تحميله فيه، وأن الأفعال المشكو منها حُمّلت على موقعين إلكترونيين متاحين للاطلاع عليهما في الأراضي اللبنانية كافة، وقد تلقاها القراء في النطاق الجغرافي اللبناني ومن ضمنه محافظة جبل لبنان،

وحيث يكون القضاء اللبناني، وتالياً قضاء تحقيق جبل لبنان مختصاً للنظر في الدعوى......"[١١١]

البند الثاني: الصلاحية الشخصية والذاتية والشاملة.

[١١١] محكمة التمييز، الغرفة الثالثة الجزائية ،قرار رقم ١٧٥ تاريخ ٢٠١٦/٥/٢٤، زياد رشدي حسين نخلة/امال احمد بو سعادة والحق العامن منشور على موقع
http://www.legiliban.ul.edu.lb/RulingView.aspx?opt&RulID=12019(last revision 14/1/2020

إن هذه الاختصاصات جاءت مكمّلة للاختصاص الإقليمي، إذ إنها تسمح بامتداد سلطان القانون الجزائي إلى خارج حدود الدولة، ويظهر دورها جلياً في جرائم المعلوماتية والإنترنت نظرًا إلى كون عناصرها غالباً ما تكون في فضاء سيبراني عابر للحدود والأقاليم.

متى تطبق الشريعة اللبنانية على الجرائم خارج حدود الدولة؟

١- مبدأ عينية النص الجزائي الصلاحية الذاتية .

يعني مبدأ عينية النص الجزائي أي تطبيقه على كل جريمة تمس مصلحة أساسية في الدولة. وذلك أياً كان مرتكبها وجنسية من ارتكبها. ولا جدال في أهمية هذا المبدأ، إذ تحرص كل دولة على مصالحها الشخصية الأساسية وتهتم في إخضاع الجرائم التي تمسها لتشريعاتها وقضائها، لأنها لا تثق باهتمام الدول الأخرى بالمعاقبة عليها.[112]

ولقد تناولت المادة ١٩من قانون العقوبات اللبناني[113] هذه الحالات دون الأَخذ بعين الاعتبار الجريمة الرقمية أو جريمة الإنترنت نظرًا إلى حداثة هذا الموضوع وهنا نطرح السؤال التالي: ألا

[112] حسني (نجيب)، شرح قانون العقوبات القسم العام، الطبعة الثالثة ٢٠٠٠، منشورات الحلبي الحقوقية بيروت لبنان ص ١٩٧

[113] المادة ١٩ من قانون العقوبات: معدلة وفقا للمرسوم الاشتراعي رقم ١١٢ تاريخ ١٩٨٣/٩/١٦ القانون ٥١٣ تاريخ ١٩٩٦/٦/٦ تطبق القوانين اللبنانية على كل من كان فاعلًا، أو متدخلًا أو محرضًا أو شريكًا (لبنانيًا كان أو أجنبي أو عديم الجنسية)، أقدم خارج الأراضي اللبنانية أو على متن طائرة أو سفينة أجنبية:

١ –على ارتكاب جرائم مخلة بأمن الدولة او تقليد خاتم الدولة او تقليد او تزوير اوراق العملة او السندات المصرفية اللبنانية او الاجنبية المتداولة شرعا او عرفا في لبنان, او تزوير جوازات السفر وسمات الدخول وتذاكر الهوية ووثائق اخراج القيد اللبنانية. على ان هذه الاحكام لا تطبق على الاجنبي الذي لا يكون عمله مخالفًا لقواعد القانون الدولي
٢–على ارتكاب إحدى الجنايات ضد سلامة الملاحة الجوية أو البحرية والمنصوص عليها في المواد ٦٤١ و٦٤٢ و٦٤٣ المعدلة من قانون العقوبات.

٣ –على ارتكاب إحدى الجرائم ضد سلامة المنصات الثابتة في الجرف القاري التابع لإحدى الدول المتعاقدة في بروتوكول روما المعقود بتاريخ ١٩٨٨/٣/١٠.

يعتبر خرق أي موقع رسمي للدولة اللبنانية والحصول على معلومات رسمية سرية من خلال القرصنة اعتداءً على سيادة الدولة اللبنانية؟ وبالتالي تنعقد الصلاحية الذاتية؟

مبدأ شخصية النص الجزائي .

لمبدأ شخصية النص الجزائي وجهان: وجه إيجابي ووجه سلبي. الوجه الإيجابي وهو الوجه الذي أخذ به القانون اللبناني، ويقصد به تطبيق القانون الجزائي على مرتكب الجريمة الذي يحمل جنسية الدولة، ولو ارتكب الجريمة خارج إقليمها. أما الوجه السلبي فهو تطبيق القانون على الجريمة التي يقع ضحيتها من يحمل الجنسية اللبنانية، وهذا ما لم ينص عليه القانون اللبناني على عكس القانون الفرنسي.

تكمن أهمية هذا المبدأ في عدم إفلات المجرم من العقاب، إذا ارتكب جريمة خارج إقليم الدولة التي يحمل جنسيتها، ثم عاد إليها بعد جريمته، وبيان ذلك أن دولته لا تستطيع – تبعاً لمبدأ الإقليمية – أن تعاقبه، لانه لم يرتكب الجريمة في إقليمها، وهي لا تستطيع تسليمه. ولا تستطيع الدولة التي ارتُكبت فيها الجريمة تنفيذ العقاب فيه كونه ليس متواجداً على أراضيها.[114]

وفي لبنان يتطلب توفر شرطان لتطبيق القانون اللبناني على جرائم الشخص العادي[115]:

---

٤ –على ارتكاب جرائم بهدف إلزام لبنان القيام بأي عمل كان أو الامتناع عنه، إذا حصل خلال ارتكابها تهديد أو احتجاز أو جرح أو قتل لبناني.

[114] حسني (نجيب)،شرح قانون العقوبات القسم العام، الطبعة الثالثة ٢٠٠٠، منشورات الحلبي الحقوقية بيروت لبنان ص ٢٠١.

[115] المادة ٢٠ من قانون العقوبات، تطبق الشريعة اللبنانية على كل لبناني، فاعلاً أو متدخلاً كان أو محرضا أقدم خارج الأراضي اللبنانية، على ارتكاب جنحة أو جناية تعاقب عليها الشريعة اللبنانية. ويبقى الأمر كذلك ولو فقد المدعى عليه أو اكتسب الجنسية اللبنانية بعد ارتكاب الجناية أو الجنحة.

المادة ٢١ –تطبق الشريعة اللبنانية خارج الأرض اللبنانية.

١ –على الجرائم التي يقترفها الموظفون اللبنانيون في أثناء ممارستهم وظائفهم أو في معرض ممارستهم لها.

١. أن يكون مرتكب الجريمة لبنانياً، ولو اكتسب الجنسية بعد ارتكاب الجرم، وهذا التحديد جاء في محله لإزاله أي التباس ممكن.

٢. أن يكون الفعل المرتكب جناية أو جنحة حسب التشريع اللبناني وليس مخالفة.

كما واشارت المادة ٢١ إلى الحالات التي تطبق فيها الشريعة اللبنانية خارج الأراضي اللبنانية عند ارتكاب الموظفين اللبنانيين ورجال السلك الدبلوماسي الجرائم في الخارج.

وحيث أن جرائم المعلوماتية عبارة عن جنح، وقد تتطور لتصبح جناية، فإن أي لبناني ارتكب في الخارج أي جرم رقمي أو معلوماتي، لا يتعلق بسيادة الدولة اللبنانية، يكون عرضة للملاحقة أمام القضاء اللبناني، إذا لم يصدر بحقه حكم مبرم في البلد حيث ارتكبت الجريمة، ولا حاجة لوجود ازدواجية في التجريم، أي تجريم الفعل المرتكَب في الدولة الاجنبية، بل ينعقد اختصاص القضاء اللبناني بكون الفعل يشكل جنايةً أو جنحةً في القانون اللبناني.

وقد أكدت الغرفة الثالثة في محكمة التمييز الجزائية ذلك، في القرار رقم ١٠٣سنة ٢٠١٣ الذي جاء فيه: "يعتبر القرار المطعون فيه واقعًا في محلّه القانوني لجهة رد الدفع بانتفاء صلاحية القضاء اللبناني للنظر في الدعوى، لأن فعل الإحتيال (مادة ٦٥٥ عقوبات) المنسوب الى المدعى عليه اللبناني الجنسية والمرتكب في الخارج تبلغ عقوبته ٣ سنوات حبس، ما يجعل من غير الضروري توافر شرط ازدواجية التجريم المفروض في المادة ٢٤ عقوبات لتطبيق الشريعة اللبنانية على الجنح الداخلة في اطار الصلاحية الشخصية للقضاء اللبناني بموجب المادة ٢٠ عقوبات والمعاقب عليها بعقوبة حبس لا تبلغ ٣ سنوات وبالتالي لا حاجة لاثبات ان القانون الاجنبي السعودي لا يعاقب على الافعال المدعى بها"[١١٦].

٢- الصلاحية الشاملة أو العالمية.

---

٢ –على الجرائم التي يقترفها موظفو الملاك الخارجي والقناصل اللبنانيون ما تمتعوا بالحصانة التي يخولهم إياها القانون الدولي العام.

[١١٦] محكمة التمييز الجزائية، الغرفة الثالثة، قرار رقم ٢٠١٣/١٠٣، "جان بو سمرا"/الحق العام و"بديع حسن".

مبدأ الصلاحية هذا يعني وجوب تطبيق النص الجزائي على كل جريمة يقبض على مرتكبها في إقليم الدولة، أيا كان الإقليم الذي ارتكبت فيه، و أيًا كانت جنسية مرتكبها[117].

ولقد ظهر هذا المبدأ بعد انتشار العصابات الدولية التي تتكون من جنسيات متعددة، والتي تتنقل بين الدول من أجل تجارة المخدرات والقرصنة، بحيث وجب مكافحة هذه العصابات من خلال تعاون الدول فيما بينها وتولي كل دولة معاقبة المجرم الذي يضبط على أراضيها دون الاكتراث إلى جنسيته. مع العلم ان مثل هذا التعاون يحتاج الكثير من التنسيق المتواصل وتبادل المعلومات بين الدول من أجل تنفيذ إجراءات الملاحقة، ومنها جمع الأدلة الرقمية وهذا ما سنتطرق إليه في القسم الثاني بشكل موسّع.

وأمام حداثة الجريمة الرقمية وسرعة ضياع الدليل الرقمي، يصبح مبدأ عالمية النص الجزائي ذا أهمية بالغة، فبدل لجوء الدول إلى التفويض القضائي من أجل جمع الأدلة الرقمية اللّازمة وملاحقة المجرم غير الموجود على أراضيها، مع ما يستنزف ذلك من وقت وجهود ضائعة وإمكانية فرار المجرم الرقمي من العقاب مستخدماً الحدود والعلاقات الدولية درعاً له، يصبح في إمكان الدولة التي تعلم أنه يتواجد على أراضيها ملاحقته ومحاكمته إحقاقاً للحق والعدالة.

وفي لبنان تناولت المادة ٢٣ الصلاحية الشاملة [118]، وشددت على توفر الشروط التالية من أجل انعقاد الصلاحية العالمية:

---

[117] حسني (نجيب)،شرح قانون العقوبات القسم العام، الطبعة الثالثة ٢٠٠٠، منشورات الحلبي الحقوقية بيروت لبنان ص ٢٠٨

[118] المادة ٢٣ من قانون العقوبات –معدلة وفقا للقانون ٥١٣ تاريخ ١٩٩٦/٦/٦ تطبق القوانين اللبنانية أيضاً على كل أجنبي أو عديم الجنسية مقيم أو وجد في لبنان، أقدم في الخارج فاعلاً أو متدخلا أو شريكاً أو محرضاً، على ارتكاب جناية أو جنحة غير منصوص عليها في المواد ١٩ (البند ١) و٢٠ و٢١، إذا لم يكن استرداده قد طلب أو قبل.

وكذلك إذا ارتكبت الجناية أو الجنحة من أي كان ضد أو على متن طائرة أجنبية مؤجرة بدون طاقم، إلى مستأجر له مركز عمل رئيسي أو محل إقامة دائم في لبنان، إذا لم يكن استرداد الفاعل قد طلب أو قبل.

١. أن يكون مرتكب الجريمة أجنبياً وإلّا أصبحنا أمام الصلاحية الشخصية.

٢. أن يكون موجودًا في لبنان ويستوي أن يكون وجوده اختيارياً أو اضطرارياً، ولقد كان النص يشترط أن يكون مقيماً قبل أن يعدلّ.

٣. ألا يكون قد طلب أو قبل استرداده من الدولة التي يحمل جنسيتها.

لقد خصصنا هذا المبحث من الفصل من أجل عرض الصلاحيات التي يطبق على أساسها سلطان النص الجزائي اللبناني، وذلك ليس زيادةً في المعلومات أو حشواً، بل للإشارة إلى المرحلة الأولية لانعقاد الاختصاص، قبل البدء بالملاحقة وجمع الأدلة الجرمية العادية منها والرقمية، وخاصةً إذا كانت الجريمة جريمة إلكترونية عابرة للحدود مثل الاستغلال الجنسي للأطفال وعرض الأفلام الإباحية لهم.

وتأكيداً لهذا الموضوع، أجريت حملة لم يسبق لها مثيل لمكافحة استغلال الأطفال جنسيًا على الإنترنت في تسع عشرة دولة، استهدفت مئة وثلاثين شخصًا موجودين في بريطانيا وأستراليا وبلجيكا ونيوزلندا والبرتغال وروسيا وأسبانيا والسويد وتايوان وتركيا والولايات المتحدة الأميركية، يشتبه في أن هؤلاء الجناة قد استخدموا منتديات المناقشة على الإنترنت، ليطلبوا ويتبادلوا الصور الإباحية عن الأطفال، وقد ذكرت الشرطة: أنها أكبر عملية تتم بالتعاون مع أجهزة العديد من الدول [119].

وبالتالي يشكل التعاون الدولي الحلقة الأساسية في مكافحة الجريمة الإلكترونية وجمع الأدلة الرقمية. ويكون على صعيدين: الصعيد الأول هو الصعيد الأمني أو الأجهزة الأمنية والصعيد الثاني هو الصعيد القضائي.

---

[119] الموقع الإلكتروني لـ"أخبار العالم"، حملة دولية لمكافحة استغلال الأطفال جنسيًا، تحقيق منشور على الرابط التالي:(http jnasrawy.com/masrawynews (last revision 9/10/2019

وهذا ما سيكون موضوعَ المبحث الأخير ملقين الضوء في الفقرة الأولى على الدوافع التقنية التي توجب التعاون الدولي، من أجل جمع الدليل الرقمي، وكيف يتبلور هذ التعاون على الصعيد الشرطي والقضائي. وفي الفقرة الثانية نتناول إتفاقية بودابست للجريمة الإلكترونية التي نظمت بشكل كبير، الأطر اللازمة للمساعدة القانونية المتبادلة في المجال الرقمي.

<u>المبحث الثاني</u>: أهمية التعاون الدولي في عملية جمع الدليل الرقمي

أدّت السهولة المتزايدة لانتقال المعلومات الرقمية في أرجاء العالم إلى ازدياد خطر الجرائم التقليدية وخاصةً الرقمية العابرة للحدود، ففي هذا العالم الذي يتّسم بالترابط المستمر، لا يمكن لأيِّ بلد أن ينجح وحده في مكافحة الجريمة على نحو فعّال.

ولهذا فإنَّ التعاون بين الدول على منع الأعمال الجرمية على أنواعها ومكافحتها بات اليوم على درجة عالية من الأهمية. ولم يعد التعاون بين الدول بسرعة وبفعالية خياراً يحتمل الأخذ والرد بل أصبح ضرورة حتمية إذا كانت هناك رغبة فعلية في تحقيق الأمن والأمان. وذلك لا يتم إلا من خلال المعاهدات والبروتوكولات الدولية العالمية.

وتوفّر هذه الأخيرة أدوات وآليات قضائية أساسية تمكّن السلطات الوطنية من إجراء تحقيقات فعّالة عابرة للحدود ومن الحرص على عدم حصول المشتبه فيهم على ملاذ آمن.

وتركّز هذه المعاهدات على التعاون الدولي من وجهة نظر العدالة الجزائية، أي تنفيذ التحقيقات والملاحقات الجزائية عندما تنطوي الجرائم المرتكبة على عنصر خارجي.

ومن أهم ما تركّز عليه في القضايا الجزائية المتعارف عليها من خلال ممارسات الدول ومبادئها، هي تسليم المجرمين والمساعدة القانونية المتبادلة.

لا مشكلة عند أي دولة بعد انعقاد اختصاصها، من القيام بإجراءات الملاحقة وجمع الأدلة العادية والرقمية إذا وَجدت هذه الأخيرة في إقليمها. أما المشكلة فهي عند وجود الأدلة وخاصةً الرقمية خارج إقليمها. ما العمل في مثل هذه الحالة ؟ إذ إنه يمنع أن تباشر أي دولة إجراءات الملاحقة في أي دولة أخرى قبل موافقتها احتراماً لمبدأ السيادة. لذلك لا بُدّ من التعاون بين الدول بشكل فعال وسريع تناسباً مع سرعة انتقال المعلومات الرقمية وإمكانية ضياع الأدلة.

ومن الناحية النظرية والعملية هناك طريقتان للتعاون الدولي في المسائل الجزائية:

١- تسليم المجرمين

٢- المساعدة القانونية المتبادلة مثل نقل الإجراءات الجزائية، تنفيذ الأحكام الصادرة في بلد أجنبي، الاعتراف بالأحكام الجزائية الصادرة في بلد أجنبي، مصادرة عائدات الجريمة، جمع وتبادل المعلومات بين أجهزة الاستخبارات[120].

وفي سبيل البقاء في موضوع بحثنا لن نتطرق إلى العناوين التي لا تعنى بجمع الدليل الرقمي مثل تسليم المجرمين والاسترداد، وفي المقابل نعرض في هذا المبحث كيف يمكن التواصل بين الدول من أجل الحصول على الأدلة الرقمية ومدى فاعلية نظام التعاون القائم حالياً.

يتجلى هذا التعاون في مستويين اثنين: الأول بين الأجهزة القضائية في الدول أو ما يعرف بالمساعدة القانونية المتبادلة التي ترعاها الاتفاقيات والصكوك الدولية، والثاني بين الأجهزة الأمنية في الدول عبر قنوات عديدة قبل الوصول إلى طلب المساعدة القانونية الدولية، أي في المراحل الأولية من التحقيق، وهنا يبرز دور المنظمة الدولية للشرطة الجزائية(الإنتربول) موضوع الفقرة الأولى.

والجدير ذكره أن أمام أدلة رقمية موجودة في عالم رقمي تقني متطور، سريع التغير والتقلب، يصبح اعتماد أساليب التعاون التقليدية بين الدول أمرًا بطيئًا جدًا لا يتناسب مع سرعة اختفاء الدليل الرقمي. لذلك كان لا بُدّ من إيجاد وسيلة أكثر تطورًا وسرعةً للتعامل مع جمع الأدلة الرقمية عبر الدول، تجلت بإتفاقية بودابست للجريمة الإلكترونية التي وضع قواعدها مجلس أوروبا عام ٢٠٠١ والتي تعتبر الآن الدليل الأهم في اعتماد المساعدة القانونية المتبادلة بين الدول في هذا المجال، ولكن لبنان ما زال حتى اليوم غير موقِّع عليها، وهذا الموضوع يبحث في الفقرة الثانية من هذا المبحث.

---

120 مكتب الأمم المتحدة المعني بمكافحة المخدرات والجريمة – برنامج التدريب القانوني على مكافحة الإرهاب

البند الأول: طلبات المساعدة القانونية بين الدول ودور الإنتربول

التعاون الدولي في استرداد المجرمين بعد تجريم المشتبه فيه أو المتهم لا يدخل كما سبق وذكرنا ضمن بحثنا، أما سبل التعاون الدولي أثناء الملاحقة الجزائية، وعند اضطرار الدولة إلى البحث عن الأدلة وخاصةً الرقمية في دولة أخرى فهذا يدخل صلب موضوعنا.

وهنا ينقسم البحث إلى قسمين:

الأول يشمل إمكانية تواصل الأجهزة الأمنية لكل دولة في ما بينها من دون الحاجة إلى اتباع قواعد المساعدة القانونية الدولية بين الدول، وهو أمر محبذ كثيرًا عند التعامل مع الأدلة الرقمية، أو التواصل مع الجهة الخاصة المعنية بحفظ الدليل الرقمي كالشركة المخدمة مثلاً.

والثاني يشمل قيام الدولة بإرسال ما يعرف بطلبات المساعدة القانونية إلى الدول الأخرى (إنابة قضائية) بغية تكليفها، وحسب قوانينها الداخلية، بالقيام بإجراءات الملاحقة القانونية اللّازمة واعلامها بالنتيجة.

لنأخذ على سبيل المثال، بعد توقيف مشتبه به لبناني بالتعامل مع منظمات إرهابية عبر الإنترنت، وتقديم المساعدات اللّازمة لها، تبين أن هناك محادثات قد حصلت عبر تطبيق الـ whatsup أو ال facebook مع منظمات إرهابية أجنبية، ولكنه قام بمسحها عن حاسوبه المصادر أو هاتفه الخاص. ما هي الإجراءات القانونية المطلوبة من أجل الحصول على مضمونها؟

رغم بساطة هذه الحالة، إلّا أنَّها تشكل الكثير من الصعوبات أمام القضاء اللبناني والضابطة العدلية من أجل الحصول على مضمون المحادثات التي تُرسل عبر تطبيق "الواتساب" (كدليل رقمي)، مع العلم أن المخدم الرئيسي لأغلب وسائل التواصل موجود في دول أجنبية وخاصةً في الولايات المتحدة الأميركية.

فيكون القضاء اللبناني في هذه الحالة أمام حلّين: الأول يتحدد بتواصل الأجهزة الأمنية، أي قوى الأمن الداخلي في لبنان، مع الأجهزة الأمنية الأجنبية حيث الدليل أو المشتبه فيه، أو مع الشركة

الخاصة الأجنبية صاحبة التطبيقات، وشرح الحاجة الملحة للحصول على مضمون المحادثات، وانتظار الرد منها آخذين بعين الاعتبار، حِرص الشركة على الخصوصية الفردية وعدم انتهاكها.

والحل الثاني يتحدد بمخاطبة الدولة المضيفة مثلاً الولايات المتحدة من أجل تفويضها قضائياً القيام بإجراءات الملاحقة الجزائية، وجمع الأدلة الرقمية نيابةً عنها، وهذا ما يسمى بالمساعدة القانونية المتبادلة التي نصت عليها العديد من الاتفاقيات الدولية التي سميت بال M.L.A.T اختصار ل"Mutual Legal Assistance Treaty"[121].

التواصل بين الأجهزة الأمنية في ما بينها أو مع الشركة المقدمة:

شهدت السنوات الأخيرة توسّعاً كبيراً في التعاون بين الأجهزة الأمنية وخاصةً الاستخبارات، ويتجلى ذلك في مكافحة جرائم الإرهاب والجريمة المنظمة، التي تستوجب قدراً كبيراً جداً من عمليات جمع المعلومات وتبادلها.

غير أنَّ هذا الشكل من أشكال التعاون الدولي لا يعدّ معادلاً للمعاهدات والاتفاقيات الدولية. إذ لا توجد بشأنه معاهدة سارية المفعول، كما في حالة تسليم المطلوبين، أو المساعدة القانونية المتبادلة، كما أنه لم يُدرج في المعاهدات المتصلة بالمساعدة القانونية المتبادلة.

وتتناول كل من إتفاقية الأمم المتحدة لمكافحة الجريمة المنظَّمة وإتفاقية الأمم المتحدة لمكافحة الفساد التعاون الشرطي الدولي ولكنهما لا تنظمانه. ولكن هذه الممارسات، نظرًا لكونها غير منظمة على الصعيد الدولي وغير مراقبة عموماً على الصعيد الوطني من قبل السلطات القضائية عند تنفيذها

---

[121] European Convention on Mutual Assistance in Criminal Matters,European Convention on the International Validity of Criminal Judgments,Inter-American Convention on Mutual Assistance in Criminal Matters,United Nations Convention against Transnational Organized Crime…

خارج الإقليم الوطني، تفرض تحديات من حيث الفاعلية واحترام الحق في حرمة الحياة الشخصية، مع العلم أنها تعد من الوسائل الأسرع في تبادل المعلومات وخاصةً الرقمية منها.

ولعل أهم أوجه التنسيق والتعاون بين الأجهزة الأمنية في الدول، يمرّ عبر المنظمة الدولية للشرطة الجنائية أو ما يعرف بالإنتربول.

ما هو الإنتربول وما هي مهامه على صعيد جمع الأدلة الرقمية؟

الإنتربول منظمة حكومية دولية تضمّ مئة واربعة وتسعين بلداً عضواً، ويتألف من **الأمانة العامة** للإنتربول التي تعنى بتنسيق الانشطة اليومية لمكافحة مجموعة من الجرائم، ويديرها الأمين العام. يعمل في الأمانة العامة ضباط من الشرطة والمدنيين، وهي تتخذ من "ليون" في فرنسا مقراً لها، ولها مجمّع عالمي للابتكار في سنغافورة والعديد من المكاتب الفرعية في مناطق مختلفة من العالم.

يشكل **المكتب المركزي الوطني** للإنتربول، في كل بلد نقطة الاتصال الأساسية للأمانة العامة والمكاتب المركزية الوطنية الأخرى. ويتولى ضباط الشرطة الوطنية إدارة المكتب المركزي الوطني، ويكون الأخير عادة تابعاً للوزارة الحكومية المسؤولة عن العمل الشرطي.

واخيراً **الجمعية العمومية**، وهي الهيئة الإدارية العليا التي تجمع ممثلي البلدان المنضمّة كافة مرة في السنة لاتخاذ القرارات.[122]

يسعى الإنتربول إلى ضمان حصول أجهزة الشرطة في أرجاء العالم على الوسائل كافة والخدمات اللّازمة لتأدية مهامها بفاعلية. ويوفر الدعم لعمليات التحقيق، عبر تقديم بيانات مفيدة، وقنوات اتصال آمنة. وتساعد هذه المجموعة المتنوعة من الأدوات والخدمات موظفي الشرطة في الميدان على فهم اتجاهات الجريمة، وتحليل المعلومات، وتنفيذ العمليات، وتوقيف أكبر عدد ممكن من المجرمين في نهاية المطاف.

---

[122] https://www.interpol.int/ar/3/3 (last revision 20/12/2019)

ويقدم مركز العمليات والتنسيق الدعم على مدار الساعة للبلدان الأعضاء، باللغات الرسمية الأربع للمنظمة، وهي الإسبانية والإنكليزية والعربية والفرنسية. فضلاً عن تمكين الدول من تبادل البيانات وخاصةً الرقمية، المتعلقة بالجرائم والمجرمين والوصول إليها، ويقدم الدعم الفني والميداني بمختلف أشكاله عبر ما يُعرف بالمنظومة العالمية للاتصالات الشرطية.

كما وإن منظمة الإنتربول تدير في الوقت الراهن حوالي سبعة عشرة قاعدة بيانات شرطية، تحتوي على معلومات عن الجرائم والمجرمين (كالأسماء وبصمات الأصابع وجوازات السفر المسروقة)، والتي يمكن للبلدان الاستفادة منها بشكل فوري. وتقدم أيضًا الدعم في التحقيقات عن طريق تحليل الأدلة الجزائية، والمساعدة في تحديد مكان الفارّين من العدالة في جميع أنحاء العالم. ويُعد التدريب جزءاً بارزاً في الكثير من المجالات حتى يصبح الموظفون ملمّين بكيفية الاستفادة من خدماتنا بشكل فعال.

وبالتالي يمكن حصر عمل منظمة الإنتربول في ثلاثة مجالات عالمية الأكثر إلحاحاً اليوم، وهي: الإرهاب، والجريمة السيبرانية، والجريمة المنظمة:

- **مكافحة الإرهاب** – منع الأنشطة الإرهابية، عبر الكشف عن هوية أعضاء الشبكات الإرهابية والمنتسبين إليها، وتقويض العوامل الرئيسية التي تمكنهم من تنفيذ أنشطتهم: السفر، والتنقل، واستخدام الإنترنت، والأسلحة والمواد، والتمويل.

- **الجريمة السيبرانية** – الجرائم التي تطال الحواسيب ومنظومات المعلومات، وتكافح المنظمة أيضًا الجرائم التي يسهل الإنترنت ارتكابها منها الاحتيال المالي واستخدام الإرهابيين لشبكات التواصل الاجتماعي وغيرها.

- **الجريمة المنظمة والناشئة** – مكافحة الشبكات الإجرامية العابرة للوطنية وشل حركتها، وكشف التهديدات الإجرامية الناشئة وتحليلها والتصدي لها.

ولقد تبنى الإنتربول "فكرة المنظومة العالمية الجديدة للاتصالات" Interpol's global Police Communications System لتوفير المزيد من السرعة والأمن في تبادل البيانات الحسّاسة بين

الهيئات الشرطية في دول العالم من أجل التصدي بفاعلية أكبر للجرائم المذكورة أعلاه.[١٢٣] كما وادرك الإنتربول أهمية التعاون مع القطاع الخاص، وضم جهوده إلى جهود شركة Microsoft لدعمها ومساعدتها في إطلاق البرنامج العالمي للحماية من الفيروسات الكمبيوترية[١٢٤].

وبرز دور اضافي لهذه المنظمة بعد انتشار فيروس كورونا COVID-19 في العالم أوائل عام ٢٠٢٠، وهو اعطاء الإرشادات لضباط وعناصر الشرطة لكيفية حماية النفس في بيئية معرضة للخطر الفيروسي، بالإضافة إلى تحذير مستخدمي الإنترنت من العمليات الإحتيالية التي تتم عبر الإنترنت مثل بيع معقمات غير صالحة أو طلب مبالغ نقدية لمعالجة أحد المصابين بالفيروس.

والجدير ذكره هنا، أن دور الإنتربول في الاتحاد الأوروبي محدود جداً بسبب وجود منظمات أوروبية أخرى تعنى المهام نفسها ويكون هدفها التنسيق بين الدول الأعضاء في الاتحاد الأوروبي مثل:

١- **قنوات الشنغن** (Les canaux Shengen) التي تضمن تبادل المعلومات الرقمية وتعميم وتنفيذ مذكرات التوقيف الأوروبية وغيرها بين الدول الأوروبية، ومرد ذلك التركيز على فكرة مرور المعلومات والتوجيهات عبر النظام المعلوماتي شنغن C.S.I.S هو كأمر إلزامي للدول الأعضاء[125].

٢- **منظمة EUROPOL**[١٢٦] **او مكتب الشرطة الأوروبية:** هي وكالة تطبيق القانون الأوروبية، وظيفتها حفظ الأمن في أوروبا، عن طريق تقديم الدعم للدول الأعضاء في الاتحاد الأوروبي في

---

[١٢٣] الخوري (جنان)، الجرائم الاقتصادية الدولية والجرائم المنظمة العابرة للحدود، الطبعة الأولى، مكتبة صادر ناشرون، لبنان، سنة ٢٠٠٩ ص ٤٤٦.

[١٢٤] المرجع نفسه ص٤٥٠

[125] Habib , **Le droit pénal libanais à l'épreuve de la cybercriminalité** , op.cit p340

[126] https://www.europol.europa.eu (last revision 5/1/2020)

مجالات مكافحة الجرائم الدولية الكبيرة والإرهاب، وخاصةً الجرائم الرقمية وتبادل المعلومات، مقرها لاهاي في هولندا وهي شبيهة جدًا بالإنتربول.[127]

ولقد أثمر التعاون بين هذه المنظمة والإنتربول نجاحًا في عمليات دولية بمشاركة العديد من دول العالم منها عملية "القناة الكبيرة" و"Operation Maxim" المتعلقة بالإتجار بالبشر[١٢٨].

٣- **جهاز العدالة الأوروبية (Eurojust)** وهو أيضًا تابع للاتحاد الأوروبي ويعنى بالتعاون والتنسيق القضائي بين الدول الأوروبية وقد يطلب من بعض الدول البدء بالملاحقات والتحقيقات أو تزويده بنتائجها. مقره أيضًا لاهاي في هولندا[١٢٩].

وفي كل ماسبق ، تتبين رغبة أغلب الدول بتفعيل التنسيق والتعاون القانوني بين الأجهزة الأمنية قبل اللجوء إلى طلبات المساعدة القانونية التي تحتاج إجراءات أكثر دقة وتعقيدًا. ولقد أنشئ في لبنان مكتب الإنتربول تابع لوحدة الشرطة القضائية يعنى بالتنسيق الدائم مع منظمة الشرطة الدولية الجزائية من أجل توفير السرعة في تبادل المعلومات وخاصةً الرقمية منها.

كما وأنه وقبل الوصول إلى طلبات المساعدة القانونية الدولية، للدولة في حال وجود الدليل الرقمي خارج إقليمها، أن تراسل الشركة المخدمة أو مزودة الخدمة في الخارج من أجل الوصول إلى حركة بيانات رقمية لمشتبه به أو لبيانات شخصية رقمية، فإذا وافقت الشركة أو الشخص على القيام بذلك فلا حاجة إلى تقديم طلبات المساعدة القانونية للدولة حيث توجد هذه الشركة أو الشخص.

---

[127] Habib , **Le droit pénal libanais à l'épreuve de la cybercriminalité** , op.cit p341.

[١٢٨١٢٨] الخوري ، **الجرائم الاقتصادية الدولية والجرائم المنظمة العابرة للحدود**، مرجع سابق ص ٤٥٦.

[129] www.eurojust.europa.eu (last revision 4/12/2019)

وهذا التواصل بين الاثنين قد يكون عبر البريد الإلكتروني أو عبر أي وسيلة اتصال أخرى توفر سرعة الإرسال وسرعة الرد. وهنا نأخذ على سبيل المثال القواعد التي وضعتها الولايات المتحدة في هذا الصدد: موضوع الحفاظ على بيانات الحاسوب المخزنة يمكن للدول الاتصال مباشرة مع مكاتب مزودي الخدمات الموجود في الدول الأجنبية وإذا وافق المكتب أو الشركة على القيام بحفظ البيانات الرقمية لصالح الدولة الطالبة، فلا يكون من الضروري تقديم طلب إلى السلطات الأميركية خاصةً وإن أغلب مزودي الخدمات الذين مقر شركتهم في الولايات المتحدة، لهم أيضًا فروع في دول أجنبية أخرى[130].

المساعدة القانونية المتبادلة والإنابة القضائية

الإنابة القضائية هي عبارة عن طلب موجه من السلطات القضائية في دولة ما إلى الجهات القضائية في دولة أخرى، بغية القيام نيابةً عنها ولحسابها بالعديد من إجراءات الملاحقة الجزائية، ويشمل ذلك الاستجواب، سماع الشهود، توقيف المشتبه فيهم بشروط معينة، والرفع أو الاستحصال على الأدلة الرقمية[131]وغيرها من إجراءات الملاحقة الجزائية.

ولا بُدّ في هذه الحالة من اتباع أسس قانونية، ترعى هذا التعاون الدولي بين الدول في المسائل القانونية، وكثيرًا ما تستند طلبات المساعدة القانونية المتبادلة، من الناحية العملية، إلى المعاهدات الثنائية والمتعدّدة الأطراف القائمة بين دول عديدة على الصعيد الثنائي والإقليمي والدولي:

- المعاهدات العالمية لمكافحة الإرهاب، التي تتبادل بموجبها الدول الأطراف أكبر قدر ممكن من المساعدة القانونية، في إطار التحقيقات والمحاكمات الجزائية المتصلة بالجرائم التي تستهدفها تلك المعاهدات.

[130] مكتب الشوؤن الدولية، القسم الجزائي، وزارة العدل الاميركية، دليل موجز للحصول على المساعدة القانونية المتبادلة في الامور الجزائية ص٤

[131] Habib, **Le droit pénal libanais à l’épreuve de la cybercriminalité**, op.cit p329

- الصكوك الأخرى التي تمّ وضعها على الصعيد العالمي بشأن المسائل الجزائية، ومنها بصفة خاصة **إتفاقية الأمم المتحدة لمكافحة الجريمة المنظَّمة(باليرمو ٢٠٠٠) وبروتوكولاتها الثلاثة**[١٣٢] **وإتفاقية الأمم المتحدة لمكافحة الفساد(ميريدا ٢٠٠٣)**[١٣٣]

كما وإنَّ طلب المساعدة القانونية المتبادلة أو توفيرها، قد لا يشترط وجود معاهدة ما، وإن كانت الدول تستحسن عموماً إسناد طلباتها إلى معاهدةٍ ما. فطلب المساعدة القانونية المتبادلة يمكن أن يستند أيضًا إلى مبادئ المعاملة بالمثل أو المجاملة، وهي مبادئ تدعمها التشريعات الداخلية.

وتجدر ملاحظة أنَّ هاتين الاتفاقيتين المشار إليهما أعلاه، تتضمّنان أحكاماً شديدة التفصيل بشأن المساعدة القانونية المتبادلة، حتى أنهما يوصفان أحياناً بأنهما "معاهدتان مصغَّرتان للمساعدة القانونية المتبادلة". لا بُدّ لنا من عرض بعض ما جاء فيها نظرًا للأهمية الموجودة:

- يجوز طلب المساعدة القانونية المتبادلة التي تقدَّم من الدول لأي من الأغراض التالية:

الحصول على أدلة أو أقوال أشخاص؛ تبليغ المستندات القضائية؛ تنفيذ عمليات التفتيش والحجز والتجميد؛ فحص الأشياء والمواقع؛ تقديم المعلومات والمواد والأدلة وتقييمات الخبراء؛ تيسير مثول الأشخاص طواعية في الدولة الطرف الطالبة.

- تُقدم الطلبات كتابة أو، حيثما أمكن، بأي وسيلة كفيلة بأن تنتج سجلا مكتوباً، بلغة مقبولة لدى الدولة الطرف متلقية الطلب، وفي ظروف تتيح لتلك الدولة الطرف أن تتحقق من صحته. يتعين إبلاغ الأمين العام للأمم المتحدة باللغة أو اللغات المقبولة لدى الدولة الطرف وقت قيام كل دولة طرف بإيداع صك تصديقها على هذه الإتفاقية أو قبولها أو

---

[١٣٢] اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر الحدود – ١٥ تشرين الثاني ٢٠٠٠ – الجمعية العامة– الدورة الخامسة والخمسون العادية– البند ١٠٥من جدول الاعمال–(A/RES/55/25) – ٥٥/٢٥

[١٣٣] اتفاقية الامم المتحدة لمكافحة الفساد – الجمعية العامة – قرار ٤/٨٥ –٣١ تشرين الأول ٢٠٠٣ –الدورة الثامنة والخمسون – البند ١٠٨ من جدول الاعمال–A/RES/58

إقرارها أو الانضمام إليها. أما في الحالات العاجلة، وحيثما تتفق الدولتان الطرفان على ذلك، فيجوز أن تقدَّم الطلبات شفويًا، على أن تؤكَّد بالكتابة لاحقاً.[134]

- يتضمن طلب المساعدة القانونية المتبادلة:

١. هوية السلطة مقدمة الطلب؛

٢. موضوع وطبيعة التحقيق أو الملاحقة أو الإجراء القضائي الذي يتعلق به الطلب، واسم ووظائف السلطة التي تتولى التحقيق أو الملاحقة أو الإجراء القضائي؛

٣. ملخصا للوقائع ذات الصلة بالموضوع، باستثناء ما يتعلق بالطلبات المقدمة لغرض تبليغ مستندات قضائية؛

٤. وصفا للمساعدة الملتَمسة وتفاصيل أي إجراءات معينة تود الدولة الطرف الطالبة اتباعها؛

٥. هوية أي شخص معني ومكانه وجنسيته، حيثما أمكن ذلك؛

٦. الغرض الذي من أجله تلتمس هذه التدابير والأدلة.

لم يلحظ قانون أصول المحاكمات الجزائية اللبناني أي شيء بشأن التفويض القضائي، بل نستنتج الممارسة الأفضل له في قانون أصول المحاكمات المدنية، من خلال مواد متعددة وموزعة تعنى فقط بإجراءات للاستخدام الداخلي[135]. و لكن يفهم منها أن القضاء اللبناني يعترف بالأدلة المرفوعة في الخارج حسب القانون الأجنبي، بحيث يمكن تفويض محكمة أجنبية بإجراءات الإثبات.

---

[134] برنامج التدريب القانوني على مكافحة الإرهاب ، النميطة رقم ٣ التعاون الدولي ، في المسائل الجزائية المتعلقة بمكافحة الإرهاب، الأمم المتحدة نيويورك، ٢٠١٢

[135] **أصول محاكمات مدنية المادة ١٣٥**– للمحكمة أن تأمر من تلقاء نفسها بإجراء أي تحقيق استكمالاً لما تذرع به الخصوم من الأدلة .

البند الثاني: إتفاقية "بودابست" للجريمة الرقمية ضمانة للتعاون الدولي الفعال

رغم أهمية الإنابة القضائية بتفعيل التعاون الدولي، والصورة الجيدة التي تنعكس من خلال ثقة القضاء اللبناني بالقضاء الاجنبي الّا أنَّ مقتضيات الجريمة الإلكترونية والأدلة الرقمية تجعل من الإجراءات التقليدية للتعاون القضائي، غير فعالة:

أولاً : هناك وقت طويل جدًا بين إرسال الطلب إلى القضاء الأجنبي وبين الحصول على النتيجة المرجوة من هذا التفويض، بسبب البطء في النظام الدولي القائم، وانتظار قبول الدولة متلقية الطلب ومباشرة العمل ما يتنافى مع طبيعة الأدلة الرقمية.

ثانياً: قد تؤدي طلبات رفع الأدلة الرقمية إلى انتهاك الحقوق المنصوص عنها في إطار الحفاظ على خصوصية الحياة الخاصة للأفراد، ما يتعارض مع قوانين الدولة متلقية الطلب، وبالتالي قد ترفض هذه الدول تقديم المساعدة القانونية اللّازمة.[136]

من هنا كان لا بد من ايجاد وسيلة، تضمن الدول من خلالها، وجود آليةٍ ما من أجل تفعيل التعاون الدولي والمساعدة القانونية، في مجال الدليل الرقمي والجرائم الرقمية، نظرًا إلى التعقيد التقني الذي يميز الأدلة الرقمية، ونظرًا إلى ضرورة توخي السرعة اللّازمة قبل ضياع الدليل، سيما وأن الارتكاز

تقوم المحكمة بالتحقيق بنفسها أو تنتدب أحد قضاتها للقيام به. وإذا كان المكان الواجب إجراء التحقيق فيه بعيداً عن مقر المحكمة جاز لها أن تنتدب القاضي المنفرد الذي يقع هذا المكان في دائرته. وتعين المحكمة المهلة التي يجب على القاضي المنتدب القيام فيها بمهمته.

يفصل القاضي المنتدب في الطوارئ التي تنشأ أثناء التحقيق. ويعترض على قراراته أمام المحكمة المنتدبة دون أن يكون للاعتراض أثر موقف لسير التحقيق

المادة ١٤٠– تخضع إجراءات الإثبات لقانون القاضي الذي تتم أمامه، ومع ذلك يعتد بإجراءات الإثبات التي تمت في دولة أجنبية إذا كانت مطابقة لأحكام القانون اللبناني، وإن كانت مخالفة للقانون الأجنبي. ومن الجائز إنابة محكمة أجنبية لاتخاذ إجراءات إثبات يقتضيها نظر الدعوى.

[136] Habib, **Le droit pénal libanais à l’épreuve de la cybercriminalité** op.cit p329

فقط على الاتفاقيات الدولية السابقة للتعاون الدولي والمساعدة القانونية، التي ذكرنا أهمها سابقًا، قد تكون غير فعالة، بسبب بطء الإجراءات الدولية التي تتم عبر القنوات الدبلوماسية.

ومن أجل وضع آلية قانونية موحّدة، لا تقتصر فقط على تناول مسائل القانون الموضوعي الجزائي، بل تعالج أيضًا المسائل الإجرائية الجزائية، وكذلك إجراءات واتفاقيات القانون الجزائي الدولي، جاءت الإتفاقية الدولية للجريمة السيبرانية التي وضعها مجلس أوروبا في "بودابست"، في ٢٣ تشرين الثاني٢٠٠١ وفتح باب التوقيع عليها.

ترمي الإتفاقية بشكل أساسي إلى تكييف عناصر القانون الجزائي المحلي مع الأحكام المتصلة بالجرائم في مجال الجريمة السيبرانية وتحديد الإجراءات الداخلية اللّازمة للتحقيق في هذه الجرائم ومتابعتها قضائيًا، علاوةً على الجرائم الأخرى التي ترتكب عن طريق نظام الكمبيوتر، أو التي تكون الأدلة الرقمية متصلة بها، وإلى إنشاء نظام سريع وفعال للتعاون الدولي.

نبحث في ما يلي الأطر التي طرحتها هذه الإتفاقية من أجل تأمين المساعدة القانونية (دون الاسترداد) الفعالة بين الدول، مشددين على ضرورة إنجاز لبنان ما يلزم من تشريعات داخلية وتطويرات في سبيل الانضمام إليها على وجه السرعة.

تشدد الإتفاقية على ضرورة توفير التعاون "على أوسع نطاق ممكن". وتكون المساعدة المتبادلة من حيث المبدأ واسعة النطاق، وقيودها محدودة للغاية. ثم، ينطبق الالتزام بالتعاون من حيث المبدأ على كل من الأفعال الإجرامية المتعلقة بأنظمة وبيانات الكمبيوتر، وبجمع الأدلة الخاصة بالجريمة الإلكترونية. وقد تم الاتفاق على فرض الالتزام بالتعاون في ما يتعلق بهذه المجموعة الواسعة من الجرائم لأن ثمة حاجة مماثلة إلى آليات مبسطة للتعاون الدولي في ما يتعلق بكلتا هاتين الفئتين، مع الأخذ بعين الاعتبار بعض الاستثناءات .

كما واعتبرت أن بيانات الكمبيوتر شديدة التقلب. ويمكن حذفها ببضع نقرات على لوحة المفاتيح، أو عن طريق تشغيل برامج تلقائية، ما يجعل من الصعب تتبع الجريمة، للوصول إلى مرتكبها، أو يؤدي إلى إتلاف الأدلة الرقمية الهامة. وفي حالات أخرى، قد يتأذى أشخاص أو يلحق ضرر جسيم

بممتلكات، إن لم يتم جمع الأدلة بسرعة. وفي مثل هذه الحالات العاجلة، يجب التسريع ليس فقط بالطلب، بل وكذلك بالرد.

تهدف الفقرة ٣ من المادة ٢٥ إلى تيسير التعجيل في عملية الحصول على المساعدة المتبادلة، بحيث لا تضيع المعلومات أو الأدلة الهامة بسبب حذفها قبل إعداد طلب المساعدة وإرسالها والاستجابة لهذا الطلب من خلال:

(١) تمكين الأطراف من تقديم طلبات عاجلة للتعاون عبر وسائل الاتصال السريعة (الفاكس والبريد الإلكتروني وغيرها)، بدلًا من الوسائل التقليدية البطيئة التي تنطوي على نقل الوثائق المكتوبة والمختومة عبر الحقائب الدبلوماسية أو البريد.

(٢) مطالبة الطرف متلقي الطلب باستخدام وسائل سريعة للاستجابة للطلبات في مثل هذه الظروف.[137]

وقبل المباشرة في بحث ما تضمنت الإتفاقية من تنظيم للتعاون الدولي في مجال جمع الدليل الرقمي، لا بُدّ من ذكر الدور الذي لعبته هذه الإتفاقية في وضع الأطر الأساسية والهامة لكيفية حصول التعاون، والتواصل بين الدول عند غياب أي معاهدة أو إتفاقية تتعلق بالجرائم الرقمية والدليل

---

[137] **Article 25 de la convention – Principes généraux relatifs à l'entraide :**

3–"Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication"

الرقمي. فشددت على ضرورة تطبيق بعض إجراءات وشروط المساعدة المتبادلة، في حالة عدم وجود معاهدة، أو ترتيب للمساعدة المتبادلة، على أساس تشريعات موحدة أو متبأدلة سارية بين الأطراف المقدمة والمتلقية للطلب.

ورفض القائمون على صياغة هذه الإتفاقية، إنشاء نظام عام، مختصّ بالمساعدة القانونية المتبادلة بشأن جرائم المعلوماتية، يطبق بدلًا من الصكوك والترتيبات الأخرى واجبة التطبيق، واتفقوا بدلًا من ذلك على أنه سيكون من العملي أكثر الاعتماد على أحكام معاهدات المساعدة المتبادلة العادية.

و من أبرز القواعد التي نصت عليها: إنشاء سلطات مركزية، وفرض شروط وأسباب وإجراءات حالات التأجيل أو الرفض، وسرية الطلبات، والاتصالات المباشرة.

وتركت في المقابل الحرية للدول، لاتباع قوانينها الداخلية في المسائل الأخرى، بحيث لا توجد أحكام تتناول شكل الطلبات ومحتواها، وتلقي شهادة الشهود لدى الجهات المقدمة أو المتلقية للطلب، وتوفير السجلات الرسمية أو التجارية، ونقل الشهود المحتجزين، أو المساعدة في مسائل المصادرة. وهنا لا بُدّ من شرح بعض القواعد المنصوص عنها:

سلطة مركزية لإرسال و تلقي الطلبات.

يعد إنشاء السلطات المركزية المخولة تقديم وتلقي طلبات المساعدة القانونية، سمة مشتركة من سمات الصكوك الحديثة التي تتناول المساعدة المتبادلة في المسائل الجزائية، إذ يبرز دورها بشكل خاص في ضمان الرد السريع، الذي يكون مفيدًا للغاية في مكافحة جرائم المعلوماتية، أو الجرائم المتصلة بالكمبيوتر. بحيث يكون الاتصال المباشر بين هذه السلطات أسرع وأكثر فاعلية من الإرسال عبر القنوات الدبلوماسية، ويؤدي وظيفة هامة في ضمان متابعة الطلبات الواردة والصادرة على حد سواء، وفي تقديم المشورة إلى الشركاء الأجانب المكلفين بإنفاذ القوانين بشأن اعتماد أفضل

السبل لتلبية المتطلبات القانونية لدى الطرف متلقي الطلب، وفي التعامل مع الطلبات العاجلة أو الحساسة بشكل صحيح.[138]

والجدير بالذكر هو تأكيد إتفاقية "بودابست" على إمكانية تواصل السلطات المركزية المتخصصة في كل دولة في ما بينها، بشكل مباشر توخيًا للسرعة والدقة اثناء جمع الدليل الرقمي.

---

[138] **article 27 de la Convention de Budapest :**En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des paragraphes 2 à 9 du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité,un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article.

a – Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution;

B– Les autorités centrales communiquent directement les unes avec les autres;

C– Chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe.

فرض شروط وأسباب وإجراءات حالات التأجيل أو الرفض.

يُلزم الطرف متلقي الطلب بتنفيذ الطلبات وفقا للإجراءات التي يحددها الطرف مقدّم الطلب، ما لم يكن ذلك متعارضا مع قوانينه. ويجدر التأكيد على أن هذه الفقرة لا تتعلق إلا بالالتزام باحترام الإجراءات التقنية.

وهكذا، لا يمكن على سبيل المثال، للطرف مقدِّم الطلب أن يطلب من الطرف متلقي الطلب تنفيذ عملية بحث ومصادرة لا تفي بالمتطلبات القانونية الأساسية للطرف المتلقي من أجل هذا الإجراء، أو في قضية يمكن أن تترتب عليها عواقب كارثية إذا كانت الوقائع، التي يقوم عليها الطلب، ستعلن للعموم.

لذلك، يسمح لمقدِّم الطلب بالتماس إبقاء الطلب ومحتواه سريين. ومع ذلك، لا يجوز التماس السرية إلى درجة تقوض قدرة الطرف متلقي الطلب على الحصول على الأدلة أو المعلومات المطلوبة. مثلًا عندما يلزم الكشف عن المعلومات والأدلة الحصول على أمر من المحكمة من أجل تقديم المساعدة، أو حيث يوجد احتمال اطلاع الأشخاص الذين تتوفر لديهم الأدلة الرقمية. وإذا لم يتمكن الطرف متلقي الطلب من الامتثال لطلب السرية، فإنه يعلم بذلك الطرف مقدّم الطلب، الذي يبقى لديه بعد ذلك خيار سحب الطلب أو تعديله.[139]

---

[139] فقرة ٨ من المادة ٢٧ من اتفافية بودابست ٢٠٠١ :

La partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre restent confidentiels, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée.

.

سرية الطلبات

على غرار ما سبق، لا تنطبق هذه القاعدة إلا في غياب معاهدة للمساعدة المتبادلة، أو ترتيب على أساس تشريعات موحدة أو متبادلة سارية بين الجهات المقدمة والمتلقية للطلب.

تسمح الفقرة ٢ للطرف متلقّي الطلب، عند الاستجابة لطلب المساعدة المتبادلة، بفرض نوعين من الشروط. أولهما، يجوز له أن يطلب الحفاظ على سرية المعلومات أو المواد المقدمة، مثلًا عندما تكون هوية مخبر سري مهددة. وليس من الملائم المطالبة بالسرية المطلقة في الحالات التي يكون فيها الطرف متلقي الطلب ملزمًا بتقديم المساعدة المطلوبة ،لأن ذلك من شأنه أن يقوض، في كثير من الحالات، قدرة الطرف مقدم الطلب على التحقيق في الجرائم أو محاكمتها بنجاح.

وثانيهما للطرف متلقي الطلب أن يرفق تقديم المعلومات أو المواد بشرط عدم استخدامها في تحقيقات أو إجراءات غير تلك المشار إليها في الطلب. ولكي ينطبق هذا الشرط، يجب أن يشير إليه الطرف متلقي الطلب بصريح العبارة، وإلا، لا يوجد أي قيد من هذا القبيل على استخدامها من قبل الطرف مقدم الطلب.[140]

وسنعمد إلى شرح المواد الأهم التي نصت عليها هذه الإتفاقية، وهي المواد التي تدخل في صلب التعاون من أجل جمع الدليل الرقمي بين الدول. وقد اعتبرت المواد (من ٢٩ وحتى ٣٤) اعتبرت أن التعاون بين الدول يقوم على مستويين: الأول هو عند اتخاذ التدابير الاحتياطية قبل البدء بالإجراءات الخاصة بالملاحقة الجزائية، والثاني هو عند البدء بها. لذلك نعرض في ما يلي

---

[140]**Article 28 de la convention** La partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre restent confidentiels, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée.

المستويين كل على حدة مشيرين إلى الأهمية التي تحتوي هذه المواد عليها، ليس فقط في التعاون الدولي بل أيضًا للاستئناس بها في التشريعات الداخلية.

١. **التدابير الاحتياطية قبل البدء بجمع الدليل :**

تشمل هذه التدابير:

- إما التعجيل **في المحافظة** على الأدلة الرقمية أو البيانات المخزنة في الحواسيب أو الآلة الرقمية إلى حين البدء بجمعها وتحليلها، بحيث يُقدم طلبٌ للحصول على التعجيل بحفظ البيانات المخزنة في إقليم الطرف متلقي الطلب، وتقتضي الفقرة ٣ من المادة ٢٩[141] أن تكون لكل طرف القدرة القانونية على تحقيق ذلك عبر نظام الكمبيوتر، بغية تفادي تغيير البيانات أو إزالتها أو حذفها خلال الفترة الزمنية اللّازمة، لإعداد وإرسال وتنفيذ طلب المساعدة المتبادلة للحصول على تلك البيانات. ويعتبر الحفظ تدبيرًا مؤقتًا محدودًا يُتوخى منه السرعة بشكل أكبر بكثير من تنفيذ المساعدة المتبادلة التقليدية.

وتتميز هذه العملية بالسرعة، وحماية خصوصية الشخص الذي تخصه البيانات، حيث لا يتم الكشف عنها أو فحصها من قبل أي مسؤول حكومي، حتى يتم استيفاء معايير الكشف الكامل، وفقا لأنظمة المساعدة المتبادلة العادية. وفي الوقت نفسه، يُسمح للطرف متلقي الطلب باستخدام إجراءات أخرى

---

[141] **Article 29 – Conservation rapide de données informatiques stockées**

1- Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.

لضمان الحفظ السريع للبيانات، بما في ذلك التعجيل في إصدار وتنفيذ أمر التقديم أو أمر البحث عن البيانات.

والأهم من ذلك، أنه لا يجوز للدولة متلقية الطلب، بموجب الفقرة ٥، أن ترفض طلبًا للحفظ، إلا إذا كان تنفيذه يمس بسيادتها أو أمنها أو نظامها العام أو مصالحها الأساسية الأخرى، أو عندما تعتبر الجريمة جريمة سياسية، أو جريمة ذات الصلة بجريمة سياسية. ونظرًا لمركزية هذا التدبير في التحقيق الفعال، والملاحقة القضائية للجرائم المرتكبة عبر الكمبيوتر، أو المتصلة بالكمبيوتر، تم الاتفاق على أن عدم اعتماد أي أساس آخر لرفض طلب الحفظ. و هذا ما يزيد من فاعلية المساعدة الدولية القانونية في مجال العالم الرقمي.

- التعجيل **في الكشف** عن البيانات المخزنة [142]

وكثيرًا ما يقوم متلقي الطلب، بناءً على طلب دولة ارتُكبت فيها جريمة ما، بحفظ بيانات الحركة، من أجل تتبع الإرسال إلى مصدره وتحديد مرتكب الجريمة، أو تحديد الأدلة الرقمية القاطعة. ويمكن

---

[142] Article 30 de la convention de budapest 2001 – Divulgation rapide de données conserves:

Lorsque, en exécutant une demande de conservation de données relatives au traffic concernant une communication spécifique formulée en application de l'article 29, la Partie requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la Partie requérante une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de services et la voie par laquelle la communication a été transmise.

أن يكتشف الطرف متلقي الطلب، عند قيامه بذلك، أن بيانات الحركة الموجودة في إقليمه تشير إلى أنه تم توجيه الإرسال من مقدم خدمة تقنية في دولة ثالثة، أو من مقدم خدمة في الدولة مقدمة الطلب نفسها. وفي مثل هذه الحالات، يتعين على الطرف متلقي الطلب، أن يُقدِّم على وجه السرعة إلى الطرف مقدم الطلب كمية كافية من بيانات الحركة للتمكين من التعرف على هوية مقدم الخدمة في الدولة الأخرى وتحديد مسار الاتصال من الدولة الأخرى المعنية. وإذا كان الإرسال صادرًا من دولة ثالثة، فإن هذه المعلومات ستمكن الطرف مقدم الطلب من تقديم طلب حفظها والتعجيل في المساعدة المتبادلة إلى تلك الدولة الأخرى بغية تتبع انتقاله إلى مصدره النهائي.

٢. **التعاون الدولي أثناء إجراءات الملاحقة الجزائية**

أثناء الملاحقة الجزائية وبعد تقديم الدولة الطلب بالمساعدة القانونية، ميزت هذه الإتفاقية بين الوصول إلى المعلومات والبيانات المخزنة داخل الكمبيوتر أو الهاتف، وبين النفاذ إليها من خارج حدود الدولة حيث يوجد نظام التخزين.

ففي الحالة الأولى(البيانات المخزنة) نصت المادة ٣١ من الإتفاقية على أنه يجب أن تتوفر لدى كل طرف القدرة على القيام بإجراءات البحث والمصادرة، أو التأمين والكشف عن بيانات مخزنة بواسطة نظام كمبيوتر يوجد داخل إقليمه (البحث عن بيانات الكمبيوتر المخزنة ومصادرتها التي سبق وذكرناها في القسم الأول من بحثنا).

وتطبق الفقرة ٢ أيضًا، مبدأ ضرورة تطابق أحكام وشروط تقديم هذا التعاون للأحكام والشروط المنصوص عليها في المعاهدات والترتيبات والقوانين المحلية المنطبقة، التي تحكم المساعدة القانونية المتبادلة في المسائل الجزائية. على أن يكون الرد سريعاً إذا كانت هنالك أسباب تدعو إلى الاعتقاد بأن البيانات ذات الصلة، معرضة بشكل خاص للإتلاف أو التعديل.[143]

[143] **Article 31 – Entraide concernant l'accès aux données stockées**

1- Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données

أما في الحالة الثانية أي عند الوصول من خارج الحدود إلى الأدلة الرقمية والبيانات، فالمسألة أكثر تعقيداً إذ إنها تثير السؤال التالي: متى يُسمح لدولة بالنفاذ من جانب واحد إلى بيانات الكمبيوتر المخزنة في دولة أخرى من دون التماس المساعدة القانونية المتبادلة؟

ليس من الممكن، بعد إعداد نظام شامل وملزم قانوناً، ينظم هذا المجال نظرًا لانعدام الخبرة الملموسة في مثل هذه الحالات. إلّا أنَّ المادة ٣٢ من الإتفاقية حاولت تنظيم المسألة بشكل منطقي ومعقول وسمحت بذلك في حالتين:

الأولى: عندما تكون البيانات التي يتم الوصول إليها متاحة للجمهور بشكل حر وسهل. **والثانية،** عندما يكون الطرف قد استفاد من بيانات وأدلة رقمية من خارج إقليمه عبر نظام كمبيوتر في إقليمه، وحصل على الموافقة القانونية والطوعية للشخص صاحب السلطة القانونية بالكشف عن البيانات في ذلك النظام.

---

stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.

2 – La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article 23, et en se conformant auxdispositions pertinentes du présent chapitre.

3– La demande doit être satisfaite aussi rapidement que possible dans les cas suivants:

a) il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification; ou

b) les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.

على سبيل المثال، يمكن أن يتم تخزين البريد الإلكتروني للشخص في بلد آخر من قبل مقدم الخدمة التقنية (isp)، أو أن يقوم شخص بتخزين بيانات عمدًا في بلد آخر. ويجوز لهؤلاء الأشخاص استرجاع البيانات، كما يمكنهم أن يكشفوا طوعاً عن البيانات للموظفين المكلفين بتطبيق القانون (الضابطة العدلية والقضاء)، أو أن يسمحوا لهؤلاء الموظفين بالوصول إلى البيانات، كما هو منصوص عليه في المادة، شرط أن تتوفر لهم السلطة القانونية.[144]

أما في الحالات الأخرى فليس من السهل السيطرة عليها، لا سيما وأنها قد تعتبر خرقاً لسيادة الدولة حيث البيانات مخزّنة إذ حصل الخرق دون علمها الرسمي.

و الجدير بالذكر أيضًا تمييز الإتفاقية بين نوعين من البيانات: بيانات الحركة وبيانات المحتوى.

وسبق وأن فصلنا الفرق بين الإثنين بشكل موسع. وشددت الإتفاقية على ضرورة تقديم المساعدة القانونية اللّازمة بين الدول من أجل الوصول ليس فقط إلى بيانات الحركة بشكل عام بل الوصول إليها في الوقت الحقيقي[145] خاصةً وأنه في كثير من الحالات، لا يستطيع المحققون ضمان تمكنهم

---

[144] **Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public:** Une Partie peut, sans l'autorisation d'une autre Partie :

A) accéder à des données informatiques stockées accessibles au public (source ouverte),quelle que soit la localisation géographique de ces données; ou

B) accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

[145] **Article 33 – Entraide dans la collecte en temps réel de données relatives au traffic:**

من تتبع اتصال إلى مصدره باتباع المسار من خلال سجلات الإرسالات السابقة، نظرًا إلى احتمال الحذف التلقائي لبيانات الحركة الأساسية من قبل مقدم الخدمة في سلسلة الإرسال قبل التمكن من حفظها. ولذلك فمن الأهمية بمكان أن يكون لدى المحققين، في كل طرف، القدرة على الحصول على بيانات الحركة في الوقت الحقيقي في ما يتعلق بالاتصالات التي تمر عبر نظام الكمبيوتر في أطراف أخرى.

و نحن نعتقد أن تقديم المساعدة المتبادلة على نطاق واسع في ما يتعلق بجمع بيانات الحركة في الوقت الحقيقي، لهوَ أمرٌ في غاية الأهمية، وقد يكون الأهم، لأن هذا النوع من جمع الأدلة الرقمية يعتبر أقل تطفلاً من اعتراض بيانات المحتوى أو عمليات البحث والمصادرة، ولأن جمع بيانات الحركة في الوقت الحقيقي يكون في بعض الأحيان الطريقة الوحيدة للتحقق من هوية مرتكب الجريمة ومكانه.

أما في اعتراض بيانات المحتوى[146]، ونظرًا لدقة هذا الموضوع وتعريض الحياة الخاصة والخصوصية الفردية للانتهاك وقدرته على جعل الشعوب تظن أنها مراقبة في جميع مراحل حياتها

---

1) Les Parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe 2, cette entraide est régie par les conditions et les procédures prévues en droit interne.

2) Chaque Partie accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

[146] **Article 34 – Entraide en matière d'interception de données relatives au contenu**

وتحويل الأنظمة إلى أنظمة استخباراتية، لم تتطرق الإتفاقية إلى تفاصيل حصول التعاون، وتُركت الطابة في ملعب الدول للاتفاق في ما بينها على ما تراه مناسباً.

تكثر لائحة الدول التي وقعت على تلك الإتفاقية، الّا أنَّ لبنان ليس منها، وقد يكون مردُّ ذلك لعدم قدرته تقنياً وتكنولوجياً وقانونياً، آنذاك، على استيفاء الشروط المنصوص عنها، خاصةً في مجال الحفاظ على الأدلة الرقمية واعتراض بيانات المحتوى، وتقديم المساعدة القانونية للدول الأخرى .

الّا أنَّنا نرى وبعد إقرار القانون ٨١ في ١٠-١٠-٢٠١٨ أنه أصبح من الممكن لا بل من الواجب انضمام لبنان إلى إتفاقية "بودابست"، ولا نقول هنا أن هذا القانون كافٍ، أو لا تشوبه شائبة بل إنه يحتاج إلى الكثير من التعديلات والتحسينات، ولكن لا يمكن القيام بذلك من دون الانخراط في مجال التعاون مع الدول الأخرى، ومن تبادل طلبات المساعدة، بحيث يبيِّن سير الإجراءات بحد ذاته للبنان ما يجب تعديله أو الاضافة إليه في القانون.

يستنتج من القسم الثاني أن اتباع الأصول التقنية الصحيحة في رفع الأدلة الرقمية من نظام معلوماتي موثوق وحفظها في الامكنة المخصصة وبالطرق المناسبة، يشكل العمادة الأساسية في ترسيخ نزاهتها ومصداقيتها في تبيان الحقائق. كما وأنها تعزز من قناعة القاضي وتسهل عليه تقدير الموقف للتوصل إلى الحكم المناسب والعادل.

ولا بُدّ أن يترافق ذلك مع الإلمام الكافي للجسم القضائي بالعالم الرقمي السيبراني أكان من حيث آلية العمل، او اللغة الرقمية المعتمدة من قبل الخبراء أو الضابطة العدلية.

Les Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

كما وتبرز أهمية اعتماد آلية مصادقة الشخص الثالث على البيانات الرقمية التي تستخدم كأدلة في القضايا الجزائية، من خلال الوظائف الموكلة إليها، مثل تأمين وسائل الحماية اللازمة للبيانات، والتحقق من هوية صاحبها، والتاريخ الصحيح لها، وتأمين حفظها بشكل سليم.

ونظراً إلى الامتداد الواسع للعالم الرقمي، واعتماد الاتصال والتواصل عبر الإنترنت، باتت الدول ترتكز على أنظمة تخزين للمعلومات موزعة بين العديد من الدول، فبرزت الحاجة الملحَّة إلى تحديد دقيق لقواعد الاختصاص للنظر في جرائم المعلوماتية وتطبيق القانون الجزائي الخاص بكل دولة حسب الجريمة السيبرانية المرتكبة وإلى تفعيل التعاون بين الدول من أجل خلق نظام فعّال في رفع الأدلة الرقمية وجمعها وحفظها.

يتبلور التعاون الدولي في شقين: الشق الأول يشمل التعاون الدولي بين الأجهزة الشرطية في ما بينها أو عبر المؤسسات البوليسية الدولية "كالإنتربول" و"اليوروبول" التى تعنى بنقل المعلومات الأمنية والإجراءات المتعلقة بالملاحقة الجزائية والشق الثاني يظهر من خلال طلبات المساعدة القانونية المتبادلة حيث يتم تفويض الدولة متلقية الطلب للقيام بالعديد من إجراءات الملاحقة الجزائية المتعلقة بالدليل الرقمي (التسريع في حفظ او كشف البيانات الرقمية وحركة الاتصالات ومعرفة موقع البث...).

وهذا الأمر كان الدافع الاساسي في صياغة إتفاقية بودابسست ٢٠٠١ للجريمة الرقمية التي أصبحت الدليل الأمثل للتعاون الدولي في هذا المجال حيث أنها أكدت على ضرورة إنشاء سلطة مركزية تكون معنية بتقديم وتلقي طلبات المساعدة القانونية في كل دولة، وعلى ضرورة توخي السرعة في الحصول على الرد والحد قدر المستطاع من حالات رفض التعاون او الإجابة وغيرها من الإجراءات التنظيمية من أجل ضمان السرعة والفاعلية في تبادل الأدلة الرقمية.

الخاتمة

نستنتج مما تقدم أنه وعلى صعيد الضابطة العدلية في لبنان، لا يزال التعامل مع الدليل الرقمي بحاجةٍ إلى الكثير من الجهد من أجل الوصول إلى آلية موحَّدة وفعّالة في عملية رفعه وحفظه، تضمن سلامته ونزاهته كي تزيد من قوّته الثبوتية أمام المحكمة، وذلك يشمل المراحل كافة، بدءًا بتجهيز وتدريب الأجهزة الأمنية المعنية على آلية جمع الأدلة الرقمية، وتفعيل التعاون بينها وبين القطاع الخاص، كما تبادل الخبرات وتطوير المهارات الخاصة لضباط وعناصر قوى الأمن الداخلي، في سبيل البحث عن الأدلة الرقمية، وهي العملية التي تمرّ عبر آليات رفعها من ذاكرة النظام المعلوماتي أو اعتراضها في الوقت الحقيقي، كذلك بالمراقبة الإلكترونية، لتنتهي بتوفير معايير وظروف تضمن حسن حفظه وعدم المساس به إلى حين عرضه أمام المحكمة.

ويشكّل تدريبَ الجسمِ القضائي على فهم العالم الرقمي، خطوةً أساسيّة مهمّة تُساعد القضاة في تكوين القناعة اللّازمة بالدليل الرقمي المعروض، وتقييم مدى سلامته ونزاهته من أجل قبوله أو رفضه. كذلك تظهر جلياً الحاجة إلى التطوير المستمر على الصعيد التشريعي من أجل مواكبة التطور الرقمي.

وقد جاء القانون ٨١ تاريخ ١٠-١٠-٢٠١٨ كخطوة أولى جيّدة ولو متأخرة في رحلةِ ملاءَمة التشريعات والنصوص الداخلية مع العالم الإلكتروني والرقمي لإضفاء المشروعية على إجراءات جمع الأدلة الرقمية، والحدِّ من السِجّلات في موضوع الدخول إلى أنظمة البيانات الرقمية عن بعد كما المراقبة الإلكترونية، لإشراك مزودي الخدمات التقنية في تحمّل مسؤولية الحفاظ على الأدلة الرقمية، فتسهيل الوصول إليها حين يطلب القضاء ذلك (حركة الاتصالات والبيانات ومعرفة عنوان كل مشترك وهويته وغيرها من المعلومات التي تفيد التحقيق).

كما تبرز حاجة للبنان إلى التوقيع على إتفاقية "بودابست" للمعاملات الإلكترونية، التي صدرت عن المجلس الأوروبي عام ٢٠٠١ والتي تنظم آلية التعاون الدولي في سبيل جمع الأدلة الرقمية والحفاظ عليها، رغم اختلاف التشريعات الداخلية في كلّ بلد، لأنّه في كل لحظة يكون فيها خارج الإتفاقية

سيعكس صورة للمجتمع الدولي عن عجزه، وعدم كفاءته في التعامل بالشكل المطلوب دولياً مع الجريمة الإلكترونية بشكل عام، ومع الأدلة الرقمية بشكلٍ خاص، مع العلم بأنّ القدرات البشرية والطاقات موجودة، والأجهزة الأمنية والقضائية قادرة على مواكبة ولو بالحدِّ الأدنى معظم الدول الأخرى من الناحية التقنية.

وعليه نذكر بعض المقترحات الهامة التي توصلّنا إليها والتي لا بُدّ من أخذها بعين الاعتبار في لبنان من أجل زيادة الفاعلية في التعاطي مع الأدلة الرقمية وجرائم المعلوماتية الإلكترونية :

- **تعيين وزارة العدل السلطة المركزية في لبنان** بحيث تتلقى طلبات المساعدة القانونية من الخارج بوجود مكتب مختص بالتدقيق في الطلبات الواردة، وتحديد ما إذا كان الطلب كافياً وفقاً للقانون اللّبناني، والطريقة الأنسب لتنفيذه.
- **تحويل طلبات المساعدة القانونية الواردة من الخارج إلى مدعي عام التمييز**، الذي يقرر بدوره الجهّة المناسبة لتنفيذ الطلبات، وفي هذه الحال من الأفضل أن تكون الجهّة: امّا مكتب مكافحة جرائم المعلوماتية في الشرطة القضائية، إمّا شعبة المعلومات وذلك نظرًا للخبرة التقنية والقانونية الموجودة لدى ضبّاط وعناصر هذين الجهازين، مع الحفاظ على دور مكتب الأعتدة واللوازم في المباحث الجنائية العلمية، من أجل تحليل البيانات والأدلة الرقمية.
- **التشدد في تطبيق القانون رقم ٨١** من حيث إلزام مقدّمي الخدمات على الاحتفاظ بسجلات الاتصال والحركة للمشتركين بالإضافة إلى اعتماد الدقة في الحصول على هُويات المشتركين وعناوين السكن الدقيقة والمفصّلة لهم من أجل تسهيل عملية تحديد مواقع المستخدمين حين تدعو الحاجة.
- **إجراء التعديلات اللازمة على قانون اصول المحاكمات الجزائية اللبناني** في ما يتعلق بالاثبات الإلكتروني وفرض اتباع الأصول الازمة في رفع الادلة وحفظها بشكل يضمن نزاهتها وموثوقيتها امام القضاء بالإضافة إلى توضيح كيفية تنفيذ التفتيش للنظام المعلوماتي الانتقال المكان الجغرافي أي المكان حيث يوجد فيه هذا النظام ليصار إلى تفتيشه أو امكانية إجراء ذلك من المكاتب الخاصة للضابطة العدلية من دون الانتقال.

- **إنشاء نيابة عامة رقمية مكونة من قضاة اختصاصين** خاضعين لدورات مكثّفة في موضوع العالم الرقمي الإلكتروني وتكون مهمتها منبثقة من مهام النيابة العامة الاستئنافية في الجرائم الإلكترونية، أسوةً بصلاحيات النيابة العامة المالية في الجرائم المالية.
- **وضع دليل مفصّل للحصول على المساعدة القانونية في الأمور الجزائية في الجمهورية اللبنانية،** تُذكر فيه جميع المعايير المطلوبة، بغية حفظ البيانات الرقمية، أو مصادرة الأجهزة، أو اعتراض الحزمات و بيانات الحركة في الوقت الحقيقي، وحتى الوصول إلى بيانات المحتوى، وتوزيعه على الدول عبر وزارة الخارجية اللبنانية.
- **ضرورة استحداث التعديلات اللازمة على قانون العقوبات اللّبناني** من أجل اعتبار النطاق العلوي اللبناني المنتهي ب "LB" بمثابة الإقليم اللبناني أو بحكم الأرض اللبنانية. وبالتالي تطبيق النصوص الجزائية اللبنانية على كلّ جريمة تحصل على هذا النطاق، خاصةً وأن ذلك يتّفق مع نيّة المشرّع اللّبناني في الحفاظ على سيادة الدولة البنانية على إقليمها.
- **اعتماد ما يسمى بقُضاة الوصل:** وهذه الفكرة ليست جديدة وهي متبعة من قِبل مجلس الاتّحاد الأوروبي، وهي عبارة عن تخصيص كلّ دولة قضاة معينين تكون مهامهم التنسيق مع الدول، من أجل ضمان حصول المساعدة القانونية بشكلٍ سريع ومتطابق مع القانون اللّبناني إذا كان هذا الأخير طرفًا في تقديم أو تلقي طلبات المساعدة.

وفي الختام، لقد وصل التطور التكنولوجي الرقمي إلى المجالات الحياتية كافة للأفراد، بحيث أصبح حاجة ضرورية لا يكمن الاستغناء عنها في الحياة اليومية. فمن الساعات الذكية إلى الهواتف الذكية وصولاً إلى المنازل الذكية، كلها عبارة عن بيانات رقمية، تشير بشكل واضح ومفصّل، إلى السلوك البشري اليومي، ولقد شكّل ذلك تغييرًا كبيرًا في قواعد حفظ الأمن والنظام، بحيث كلما زادت التسهيلات التقنية الرقمية للأفراد، زادت إمكانية خرق خصوصيتهم، ومراقبتهم، وزادت في المقابل التعقيدات أمام الضابطة العدلية في ملاحقة الجرائم، ورفع الأدلة الرقمية. فهل يأتي اليوم الّذي تكون فيه كل التحركات والأفعال والمحادثات الخاصة للأفراد مراقبة؟ أم سيصل التطور التقني إلى درجة تصبح معه ملاحقة الجرائم ورفع الأدلة الرقمية من قبل القضاء والضابطة العدلية في غاية الصعوبة؟

المراجع :

المؤلفات

١. الحسيني(عمار)، **التصوير المرئي والتسجيل الصوتي وحجيتهما في الإثبات الجزائي**، المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، طبعة أولى، سنة ٢٠١٧

٢. الخوري(جنان)، **الجرائم الاقتصادية الدولية والجرائم المنظمة العابرة للحدود**، الطبعة الأولى، مكتبة صادر ناشرون، سنة ٢٠٠٩.

٣. حسني(نجيب)، **شرح قانون العقوبات القسم العام**، الطبعة الثالثة ٢٠٠٠، منشورات الحلبي الحقوقية بيروت لبنان.

٤. عبد الرؤوف الخنّ (محمد) **جريمة الاحتيال عبر الإنترنت، الأحكام الموضوعية والاحكام الإجرائية**، الطبعة الأولى ٢٠١١، منشورات الحلبي الحقوقية .

٥. عيسى(ميشال)، **التنظيم القانوني لشبكة الإنترنت، دراسة مقارنة في ضوء القوانين الوضعية والاتفاقات الدولية** ،الطبعة الأولى ٢٠٠١، المنشورات الحقوقية صادر.

٦. قهوجي(علي)، **شرح قانون أصول المحاكمات الجزائية**، منشورات الحلبي الحقوقية بيروت لبنان ٢٠٠٩.

٧. نصر (فيلومين)،**أصول المحاكمات الجزائية، دراسة مقارنة وتحليل**، الطبعة الأولى٢٠١٣، المؤسسة الحديثة للكتاب.

مؤتمرات مختصّة:

١- الخوري(جنان)، مكافحة جرائم المعلوماتية، تحديات وآفاق، المؤتمر الإقليمي الأول، الطبعة الأولى ٢٠١٥، دائرة المنشورات في الجامعة اللبنانية.

المقالات:

١-الجملي(طارق)،الدليل الرقمي في مجال الإثبات الجزائي، مقال منشور على الموقع الإلكتروني www.startimes.com .

٢- رستم (هشام) جرائم المعلوماتية، أصول التحقيق الجزائي الفني وآلية التدريب التخصصي للمحققين، مجلة الأمن والقانون، كلية الشرطة دبي، العدد الثاني، السنة السابعة ١٩٩٩.

الأحكام:

١. محكمة التمييز الجزائية ، الغرفة الثالثة ، قرار رقم ١٧٥ تاريخ ٢٠١٦/٥/٢٤، زياد رشدي حسين نخلة/امال احمد بو سعادة والحق العام.

٢. محكمة التمييز الجزائية، الغرفة التاسعة، قرار رقم ١ تاريخ ٢٠١٤/١/٩ ،جان عاصي/الحق العام.

٣. محكمة التمييز الجزائية، الغرفة الثالثة، قرار رقم ٢٠١٣/١٠٣،"جان بو سمرا"/الحق العام و"بديع حسن".

٤. محكمة التمييز الجزائية، الغرفة السابعة، قرار رقم ٢٠١٣/١٠٠،"رودي سلمان/الحق العام و"صباح البدوي".

الوثائق والبرامج والمذكرات والأدلة:

١. **إتفاقية الامم المتحدة لمكافحة الفساد** – الجمعية العمومية – قرار ٨٥/٤ –٣١ تشرين الأول ٢٠٠٣ –الدورة الثامنة والخمسون – البند ١٠٨ من جدول الأعمال

٢. **إتفاقية بودابست لمكافحة جرائم المعلوماتية** – المجلس الأوروبي– الدورة ١٠٩ – ٢٣ تشرين الثاني–٢٠٠١

٣. **إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الحدود** – ١٥ تشرين الثاني ٢٠٠٠ – الجمعية العمومية– الدورة الخامسة والخمسون العادية– البند ١٠٥من جدول الأعمال.

٤. **برنامج التدريب القانوني على مكافحة الإرهاب،** النميطة ٣ التعاون الدولي، في المسائل الجزائية المتعلقة بمكافحة الإرهاب، الأمم المتحدة نيويورك، ٢٠١٢.

٥. **مذكرة الخدمة في قوى الأمن الداخلي رقم ٢٤٦/٢٠٤ش٢ تاريخ١/١١/٢٠١٦**

٦. **دليل موجز للحصول على المساعدة القانونية المتبادلة في الأمور الجزائية،** مكتب الشؤون الدولية، القسم الجنائي، وزارة العدل الأميركية.

المؤلفات الأجنبية

8. Chaer (Nidal), **La Criminalité informatique devant la justice pénale**, edition juridique sader 2004, Beirut, Liban.

9. Habib (Mohamed), **Le droit Pénal Libanais à l'épreuve de la cybercriminalité**, Edition Juridique Sader, 1ère édition 2011, Beirut, Liban.

10. Sédaillan (Valerie), droit de l'internet, 1ère edition, 1997.

1. Frayssinet(Jean), **internet et protection des données personnelles , expertises** 1998(avril)
2. Bensoussan (Alain), **un nouveau métier, le tier certificateur**, se profile sur l'internet, online Journal. 15 dec 1995

قوانين أجنبية

3. **Electronic Communications Privacy Act of 1986 (ECPA)**
4. **Federal Rules of Evidence , Rule 801 802 : Dahl's Law dictionary Compiled by Henry Saint Dhal , Hein et Dalloz 1995.**

مواقع الإلكترونية متفرقة:

1. https://www.interpol.int/ar/3/3
2. https://www.facebook.com/alkadaiyat
3. www. undoc.org
4. www.un.or.at/inicitra

5. www.uscourts.gov

6. http://www.tra.gov.lb

7. http://www.legiliban.ul.edu.lb/

8. https://www.legifrance.gouv.fr

9. http://juriscom.net

10. https://it.ojp.gov

11. https://ar.globalvoices.org/2014/04/11/334

الفهرس الصفحة